VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA PODNIKATELSKÁ
ÚSTAV INFORMATIKY

FACULTY OF BUSINESS AND MANAGEMENT
INSTITUTE OF INFORMATICS

# IMPLEMENTACE VYBRANÉ TECHNOLOGIE PRO ISP

IMPLEMENTATION OF THE SELECTED TECHNOLOGY FOR ISP

DIPLOMOVÁ PRÁCE
MASTER'S THESIS

AUTOR PRÁCE — Bc. MARTIN DOLEŽAL
AUTHOR

VEDOUCÍ PRÁCE — Ing. VIKTOR ONDRÁK, Ph.D.
SUPERVISOR

BRNO 2016

Vysoké učení technické v Brně
Fakulta podnikatelská

Akademický rok: 2015/2016
Ústav informatiky

# ZADÁNÍ DIPLOMOVÉ PRÁCE

**Doležal Martin, Bc.**

Informační management (6209T015)

Ředitel ústavu Vám v souladu se zákonem č.111/1998 o vysokých školách, Studijním a zkušebním řádem VUT v Brně a Směrnicí děkana pro realizaci bakalářských a magisterských studijních programů zadává diplomovou práci s názvem:

**Implementace vybrané technologie pro ISP**

v anglickém jazyce:

**Implementation of the Selected Technology for ISP**

Pokyny pro vypracování:

Úvod
Cíle práce, metody a postupy zpracování
Teoretická východiska práce
Analýza současného stavu
Vlastní návrhy řešení
Závěr
Seznam použité literatury
Přílohy

Seznam odborné literatury:

BIGELOW, S. J. Mistrovství v počítačových sítích: správa, konfigurace, diagnostika a řešení problémů. 1. vydání. Praha: Computer Press, 2004. 990 s. ISBN 80-251-0178-9.
CLEMM, A. Network management fundamentals. 1. vydání. Indianapolis: Cisco Press, 2007. 552 s. ISBN 1-58720-137-2.
HORÁK, J. a M. KERŠLÁGER. Počítačové sítě pro začínající správce. 5. vydání. Brno: Computer Press, 2011. 304 s. ISBN 978-80-251-3176-3.
KRETCHMAR, J. M. a L. DOSTÁLEK. Administrace a diagnostika sítí: pomocí OpenSource utilit a nástrojů. 1. vydání. Brno: Computer Press, 2004. 216 s. ISBN 80-251-0345-5.
SCHWALBE, K. Řízení projektu v IT. 1. vydání. Brno: Computer Press, 2011. 623 s. ISBN 978-80-251-2882-4

Vedoucí diplomové práce: Ing. Viktor Ondrák, Ph.D.

Termín odevzdání diplomové práce je stanoven časovým plánem akademického roku 2015/2016.

L.S.

| | |
|---|---|
| doc. RNDr. Bedřich Půža, CSc.<br>Ředitel ústavu | doc. Ing. et Ing. Stanislav Škapa, Ph.D.<br>Děkan fakulty |

V Brně, dne 30.11.2015

## Abstrakt

Diplomová práce je zaměřena na implementaci vybrané technologie ve společnosti CPU-Kocourek, s.r.o., která působí jako poskytovatel internetového připojení. Na základě teoretické části a provedené analýzy současného stavu jsou navržena dostupná řešení vhodná pro management přístupové sítě poskytovatele. Návrhová část obsahuje výběr nejvhodnějšího z nich a jeho následnou implementaci do režimu rutinního provozu.



## Abstract

The thesis focuses on implementation of selected technology within the company CPU-Kocourek, s.r.o, which provides varied internet services. Based on the theoretical part and the analysis of the current situation are proposed solutions suitable for the management of access network provider. The proposal part contains selection of the best proposal and its implementation into the routine mode of operation.



## Klíčová slova

ISP, management počítačové sítě, poskytovatel internetového připojení, monitoring, Nagios, SNMP, Linux, FCAPS model

## Keywords

ISP, computer network management, internet service provider, monitoring, Nagios, SNMP, Linux, FCAPS model

## Bibliografická citace

DOLEŽAL, M. *Implementace vybrané technologie pro ISP*. Brno: Vysoké učení technické v Brně, Fakulta podnikatelská, 2016. 79 s. Vedoucí diplomové práce Ing. Viktor Ondrák, Ph.D.

## Čestné prohlášení

Prohlašuji, že předložená diplomová práce je původní a zpracoval jsem ji samostatně. Prohlašuji, že citace použitých pramenů je úplná, že jsem ve své práci neporušil autorská práva (ve smyslu Zákona č. 121/2000 Sb., o právu autorském a o právech souvisejících s právem autorským).

V Brně dne 18. ledna 2016 ……

## Poděkování

Na tomto místě bych chtěl poděkovat vedoucímu diplomové práce Ing. Viktoru Ondrákovi, Ph.D., za jeho ochotu, čas a cenné rady. Dále bych chtěl touto cestou poděkovat společnosti CPU-Kocourek, s.r.o. za poskytnuté podklady a možnost realizace této práce.

# Obsah

**Úvod** ..... **12**

**Cíle práce** ..... **13**

**Metody a postupy zpracování** ..... **13**

**1 Teoretická východiska práce** ..... **14**

1.1 Informační společnost ..... 14

1.2 Právní aspekty ..... 14

1.2.1 Odpovědnost ISP ..... 14

1.3 Možnosti šíření sítě ISP ..... 15

1.3.1 Optické vlákna ..... 15

1.3.2 Metalické kabely ..... 17

1.3.3 Bezdrátové sítě ..... 18

1.4 Model FCAPS dle normy ISO ..... 22

1.4.1 Správa výkonu ..... 22

1.4.2 Správa konfigurace ..... 23

1.4.3 Účetní a evidenční správa ..... 23

1.4.4 Správa poruch a chyb ..... 23

1.4.5 Správa bezpečnosti ..... 24

1.5 Management ICT služeb podle ITSM / ITIL ..... 24

1.5.1 ITSM (Information Technology Service Management) ..... 24

1.5.2 ITIL (Information Technology Infrastructure Library) ..... 25

1.6 SNMP (Simple network management protocol) ..... 27

1.6.1 Základní prvky SNMP ..... 28

1.6.2 SNMP zprávy ..... 28

1.6.3 Vylepšení SNMPv2 a SNMPv3 ..... 29

1.6.4 MIB (Management information base) ..... 30

1.7 RMON (Remote Network Monitoring) ..... 31
1.7.1 Základní skupiny RMON MIB ..... 32
1.8 IP toky ..... 32
1.8.1 Využití monitorování IP toků ..... 33
1.8.2 NetFlow ..... 34
1.9 SWOT analýza ..... 35
1.10 Lewinův model změn ..... 36
1.11 Matice RACI ..... 36
**2 Analýza současného stavu ..... 38**
2.1 Představení společnosti ..... 38
2.1.1 Organizační struktura společnosti ..... 39
2.2 RACI matice ..... 40
2.3 Analýza přístupové sítě ..... 40
2.3.1 Mapa přístupové sítě ..... 41
2.3.2 Páteřní spoj Brno – Babice nad Svitavou ..... 41
2.3.3 Přístupové body ..... 42
2.3.4 Páteřní spoje v obci Babice nad Svitavou ..... 42
2.3.5 Server ..... 43
2.3.6 Router ..... 44
2.3.7 Klientská zařízení ..... 44
2.4 Prostředky pro management ..... 46
2.4.1 Informační systém ..... 46
2.4.2 Software ..... 46
2.5 Analýza prostředí ..... 48
2.5.1 Lokalita ..... 48
2.5.2 Klienti ..... 49

2.5.3 Nabízené tarify ... 49
2.6 Obchodní situace firmy ... 50
2.6.1 Trhy ... 50
2.6.2 Konkurence ... 50
2.7 SWOT analýza ... 52
2.8 Hodnocení podnikání firmy z více pohledů ... 53
2.9 Problémy při běžném provozu ... 53
2.10 Definice potřeb poskytovatele ... 54
2.11 Dostupná řešení vhodná pro management přístupové sítě ISP ... 54
2.11.1 Nagios ... 54
2.11.2 Zenoss ... 56
2.11.3 Zabbix ... 57
2.12 Shrnutí analýzy ... 58
**3 Vlastní návrh řešení ... 59**
3.1 Výběr vhodného řešení ... 59
3.1.1 Shrnutí možných řešení ... 60
3.1.2 Výběr konkrétního řešení ... 60
3.2 Technické aspekty ... 61
3.2.1 Server pro monitoring ... 61
3.2.2 Operační systém ... 62
3.2.3 Instalace systému Nagios ... 62
3.3 Definice zařízení a služeb ... 62
3.3.1 Definování zařízení (hosts) ... 63
3.3.2 Definice testované služby (services) ... 64
3.3.3 Definice kontaktů (contacts) ... 65
3.3.4 Definice časových intervalu odesílání notifikace (timeperiods) ... 65

3.4 Testovací provoz ..... 66
3.5 Režim rutinního provozu ..... 66
3.5.1 Organizační začlenění technologie, odpovědnost, pravomoci ..... 66
3.5.2 Návrh postupů pro technické oddělení (směrnice) ..... 67
3.6 Projekt zavedení dohledového systému ..... 70
3.6.1 Identifikační listina ..... 70
3.6.2 Časový harmonogram projektu ..... 71
3.7 Ekonomické aspekty ..... 72
3.7.1 Náklady ..... 72
3.7.2 Přínosy pro firmu ..... 72
**Závěr ..... 73**
**Seznam použité literatury ..... 74**
**Seznam obrázků ..... 77**
**Seznam tabulek ..... 78**
**Seznam příloh ..... 79**

# Úvod

S rozvojem informačních technologií dochází k neustálému zvyšování nároků na kvalitu a správné fungování počítačových sítí. Počítačovou síť lze definovat jako propojenou skupinu dvou a více počítačů, které používají definovaný, vzájemně dohodnutý soubor pravidel a úmluv, známé jako protokoly, tak aby mohly sdílet dostupné prostředky a zdroje. Počítačové sítě tvoří mimořádně důležitou úlohu ve světě informačních technologií. Jejich účelem je prospívat lidem a umožnit jim vykonávat jejich práci efektivněji.

Jako každá technická záležitost, tak i sítě obnáší náležitá rizika, která mohou způsobit značné problémy a také finanční ztráty. Například kolaps produkčního systému řídícího výrobu ve většině případů znamená i výpadek v samotné výrobě a tím nemalé ekonomické ztráty. Proto stále větší roli v řízení IT hrají systémy, které dělají jejich provoz bezpečnější a efektivnější - systémy řízení (managament počítačových sítí). Jde o poměrně komplikovanou záležitostí zvláště v podnicích, kde je vysoký počet systémů a zařízení (poskytovatelé internetového připojení, banky, velké výrobní korporace, telekomunikační operátoři apod.) Velice důležitou částí managementu počítačové sítě je tedy správa chyb a poruch, jedná se především o spolehlivý dohledový systém.

Úkolem dohledového systému je shromažďovat údaje z předdefinovaných zařízení a subsystémů IT infrastruktury, zpracovávat je a prezentovat způsobem, aby byla obsluha schopna dostat se k relevantním informacím včas a v potřebném rozsahu. Toho lze dosáhnout pomocí nasazení monitorovacího systému, který poskytuje sadu nástrojů a technik na získávání cenných informací o síti a jejích potřebách.

# Cíle práce

Cílem této práce je návrh implementace vybrané technologie pro management počítačové sítě u zvoleného poskytovatele internetového připojení.

Mezi dílčí cíle práce patří:

- vytvoření teoretického základu,
- konfigurace nového systému,
- vytvoření postupů pro technické oddělení (směrnice),
- zhodnocení ekonomického přínosu.

# Metody a postupy zpracování

Teoretické poznatky budou vypracovány na základě dostupné literatury nebo informací uvedených na internetu. Analytická část bude vycházet z konzultací se zaměstnanci společnosti CPU-Kocourek, s.r.o. nebo z vlastních poznatků. V návrhové části budou hlavním východiskem pro výběr nejvhodnějšího řešení požadavky definované vedoucím technického oddělení.

# 1 Teoretická východiska práce

## 1.1 Informační společnost

Pojem informační společnost označuje takovou společnost, v které informatika, počítače a mikroelektronika určují a přeměňují celý společenský systém. Vystupují jako prostředek vytvoření nových společenských struktur a zásadním způsobem mění mechanismy společenského vývoje. V praxi to znamená, že pracovníci jsou postupně nahrazováni technikou, výrobní procesy jsou digitalizovány, firmy shromažďují informace prostřednictvím informačních systémů. Dále se mění struktury řízení společností, už i malé společnosti mohou pružně reagovat na potřeby trhu. Díky počítačovým infrastrukturám jsme schopni pracovat i z pohodlí domova - na dálku, mimo kancelář (1).

## 1.2 Právní aspekty

Internet již dávno není uzavřenou sítí, ale stal se každodenním nástrojem široce používaným celou společností. Je nutné dodržovat předpisy a opatření vydané Českým telekomunikačním úřadem a řídit se zákonem č. 127/2005 Sb., o elektronických komunikacích (2).

**Poskytovatelé internetového připojení**

Jde o společnosti nebo organizace, které obvykle za poplatek poskytují přístup k internetu, zákon je označuje jako poskytovatele služeb informační společnosti. Velice často jsou nazýváni rovněž zkratkou ISP (*Internet Service Provider*) (2).

**Služba**

Je jakákoli služba informační společnosti, tj. každá služba, která se běžně poskytuje za úplatu, na dálku, elektronicky a na individuální žádost příjemce služeb (2).

### 1.2.1 Odpovědnost ISP

Na základě evropských předpisů je odpovědnost poskytovatelů upravena zákonem č. 480/2004 Sb., o některých službách informační společnosti a o změně některých zákonů. Dle míry odpovědnosti za poskytovaný obsah rozlišuje zákon tři typy

poskytovatelů, které jsou upraveny v § 3, 4 a 5. První dva typy jsou poskytovatelé zajišťující přenos a dočasné ukládání dat. Třetí typ je odpovědný za obsah informací poskytovaných uživateli, a to tehdy, mohl-li poskytovatel vzhledem k předmětu své činnosti, okolnostem a povaze případu vědět, že obsah ukládaných informací nebo jednání uživatele jsou protiprávní, nebo dozvěděl-li se prokazatelně o protiprávní povaze obsahu ukládaných informací nebo o protiprávním jednání uživatele a neprodleně neučinil veškeré kroky, které lze po něm požadovat, k odstranění nebo znepřístupnění takovýchto informací (2).

Je však velmi podstatné, že § 6 stanoví, že poskytovatelé nejsou povinni dohlížet na obsah informací a aktivně vyhledávat protiprávní obsah, protože monitorovat a filtrovat veškerý obsah, který projde přes jejich infrastrukturu, by bylo technicky velice náročné a nákladné. Zároveň by bylo narušeno ústavně garantované právo na ochranu soukromí uživatelů. Důvodem, proč je poskytovatelům vůbec nějaká odpovědnost přičítána je v tom, že by bylo velmi náročné vyžadovat nápravu protiprávního jednání pouze po tom, kdo jej způsobil. V současném pojetí je možné poskytovatele upozornit na protiprávní stav a poté mají ze zákona povinnost se problémem zabývat, případně jim může být soudem přikázána náprava protiprávního stavu. Poskytovatele navíc mohou velmi pomoci při vyšetřování, protože si vedou různé záznamy elektronických komunikací a přístupů k službám, díky čemuž je pachatel snadněji vypátratelný (2).

## 1.3 Možnosti šíření sítě ISP

ISP disponuje škálou technologií, které umožňují spotřebitelům připojit se k jejich síti, jedná se o prostředky, jejichž pomocí je komunikační signál přenášen z jednoho místa na druhé. Každé přenosové prostředí má své specifické vlastnosti a vyžaduje specializovaný hardware, se kterým je kompatibilní. Propojení může být realizováno metalickým, optickým nebo bezdrátovým vedením (3).

### 1.3.1 Optické vlákna

Tvoří prostředí pro přenos informace prostřednictvím světelného paprsku. V případě požadavku dosažení velmi velkých přenosových rychlosti, je třeba zvolit takové způsoby přenosu, které mají šířku přenášeného pásma co možná největší, tj. frekvence přenášeného signálu musí být velmi vysoká. Úkolem optického vlákna je dopravit

světelný paprsek od zdroje k detektoru s co možná nejmenšími ztrátami. Optické vlákno se skládá z jádra obaleného vhodným pláštěm. Jádro má průměr několika jednotek až desítek mikrometrů a je vyrobeno z různých druhů skla, případně plastu. V okamžiku vstupu světelného toku do optického vlákna vzniká v optickém vlákně světelný tok. Ten může být tvořen jedním, nebo několika světelnými paprsky (3).

**Obr. č. 1: Optický kabel** (Zdroj: 4)

Podle počtu přenášených paprsků se vlákna dělí na (3):

- **Jednovidová (singlemode) -** přenášejí pouze jeden světelný paprsek a jsou používána pro přenos na větší vzdálenosti. Průměr jádra je typicky do 10 mikrometrů.
- **Mnohavidová (multimode)** - přenášejí více světelných paprsků, nejčastěji jsou používána pro komunikaci na krátké vzdálenosti, jako například uvnitř budovy nebo areálu. Jsou ekonomičtější s použitím levnějších konektorů a levnějších aktivních zařízení.

**Výhody optických vláken** (3):

- **Přenos signálu na velké vzdálenosti** - nízký útlum a vysoká integrita přenášeného signálu umožňuje optickým systémem přenosy na větší vzdálenosti, než tomu je u metalických vedení. Zatímco u běžných měděných vodičů je nutné použití signálových zesilovačů, u optických tras nejsou výjimkou úseky po 100 km bez aktivních prvků, přičemž se tyto vzdálenosti novými technologiemi neustále zvyšují.

- **Větší šířka pásma, menší průměr a nižší hmotnost** - nesrovnatelně vyšší šířka pásma optického vlákna umožňuje přenos podstatně vyššího množství informací

než po celém kabelovém svazku měděných párů. Menší průměr a nižší hmotnost se projevuje i v nižších nárocích na trasu a instalační technologii.

- **Dielektricita** - optické kabely umožňují využívat přenos informace v prostředích s vysokým stupněm elektrického nebo vysokofrekvenčního zamoření. Je možné je instalovat např. v těsném sousedství s rozvody elektrické energie, přičemž nedochází k omezení přenosových nebo bezpečnostních parametrů.

- **Bezpečnost** - vzhledem k tomu, že pro přenos informace se nevyužívají elektronické principy, tak je velmi obtížné optické kabely "odposlouchávat". Jakékoliv přerušení kabelu je snadno detekovatelné.

**Nevýhody optických vláken** (3):

Mezi nevýhody patří spojování jednotlivých vláken (využívá se lepení a svařování vláken). Optická vlákna jsou velmi citlivá na mechanické namáhání a ohyby. Proto musí optický kabel, kromě jednoho či více optických vláken, obsahovat i vhodnou výplň, zajišťující potřebnou mechanickou odolnost.

### 1.3.2 Metalické kabely

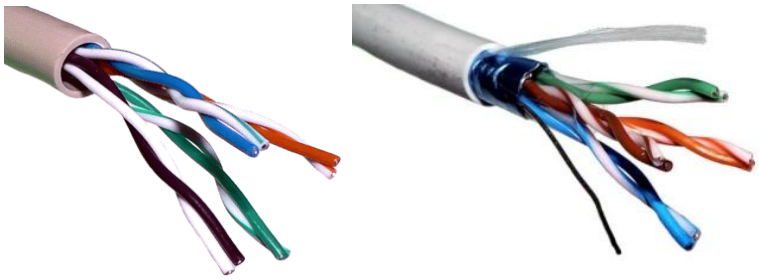
Vodiče těchto kabelů jsou tvořeny měděným drátem, který je opatřen chránícím pláštěm. Nejvíce využívaným je kabel kroucených párů (standardně 4 páry), přičemž vodiče páru jsou navzájem propleteny, zkroucení pomáhá redukovat vzájemné přeslechy, šumy z vnějšího prostředí a zároveň brání vyzařování z páru do prostředí (5).

**Tab. č. 1: Kategorie komponent metalické kabeláže a třídy použití sítě** (Zdroj: 5)

| Třída | Kategorie | Frekvenční rozsah | Použití |
|---|---|---|---|
| A | 1 | do 100kHz | Analogový telefon |
| B | 2 | do 1 MHz | ISDN |
| C | 3 | do 16MHz | Ethernet - 10 Mbit/s |
| - | 4 | do 20MHz | Token-Ring |
| D | 5 | do 100MHz | GE, FE, ATM155 |
| E | 6 | do 250MHz | ATM 1200 |
| - | 6A | do 500MHz | 10 GE |
| F | 7 | do 600MHz | 10 GE |

**Rozdělení kabelů kroucených párů dle stínění** (6):

- UTP – Unshielded Twisted Pair – nestíněný kabel, který je vhodné použít v prostředí, kde nedochází k žádnému okolnímu rušení, protože nestíněné komponenty jsou levnější na pořízení a jejich instalace je jednodušší,
- FTP – Foiled Twisted Pair - kabel, který je stíněný hliníkovou fólií,
- STP – Shielded Twisted Pair - každý pár je stíněný zvlášť a navíc je kabel stíněný i celkově,
- ISTP - kabel s individuelně stíněnými páry – páry obvykle stíněny folií, kabel opletením.



**Obr. č. 2: Kabel kroucených párů UTP / FTP** (Zdroj: )

**Konstrukce kabelu** (6):

- Provedení drát – slouží pro instalaci pevných rozvodů v horizontální sekci,
- Provedení lanko – pro propojovací kabely k připojení periférií nebo propojení rozvodů v datovém rozvaděči.

**Materiál pláště kabelu** (6):

- Standardní – PVC
- Bezhalogenový – LSOH, při hoření nevydává jedovaté plyny.
- Speciální – PE

### 1.3.3 Bezdrátové sítě

Bezdrátové sítě představují z pohledu přenosových médií moderní trend v mobilní hlasové i datové komunikaci. Pro komunikaci jednotlivých zařízení v sítí je možné použít rádiové vysílání, optické či infračervené.

Rádiové vysílání je náchylné na rušení, a to všemi prostředky, které mohou na příslušných kmitočtech pracovat. Proto je nezbytné pro spolehlivý přenos dat zvolit takové přenosové mechanismy, které zajistí vysokou spolehlivost přenosu a odolnost vůči rušení při zachování vysoké efektivity využití přenosového pásma. Dosah související s kvalitou přenosu pak omezuje jejich velikost i počet systémů, které se v rámci daného prostoru mohou nacházet, aby nedocházelo k nežádoucímu rušení. Jedním z největších problémů při rádiovém vysílání je zajištění bezpečnosti bezdrátové komunikace a směrování mezi různými sítěmi (7).

### Standard IEEE 802.11

Často používané označení Wi-Fi je zkratka pro "Wireless Fidelity " a představuje zpřesnění standardu IEEE 802.11. Tato norma má řadu dalších variant, které se liší parametry a schopnostmi sítí. Správu norem má na starosti WiFi Aliance, neziskové sdružení několika set zainteresovaných společností. Wi-Fi bylo původně určeno jako náhrada metalických rozvodů místních sítí, avšak ještě více se stalo oblíbeným způsobem přístupu k internetu. Spoje na bázi Wi-Fi mohou být typu Point to Point, Bridge a nebo Point to Multipoint (8).

V rámci normy 802.11 existuje mnoho standardů, z nichž ty nejvýznamnější jsou uvedeny v následující tabulce.

**Tab. č. 2: Standardy IEEE 802.11** (Zdroj: 7)

| **Přehled standardů IEEE 802.11** | | | |
|---|---|---|---|
| **Standard** | **Pásmo [GHz]** | **Max. rychlost [Mbit/s]** | **Fyzická vrstva** |
| původní IEEE 802.11 | 2,4 | 2 | DSSS |
| IEEE 802.11a | 5 | 54 | OFDM |
| IEEE 802.11b | 2,4 | 11 | DSSS |
| IEEE 802.11g | 2,4 | 54 | OFDM |
| IEEE 802.11n | 2,4 nebo 5 | 600* | OFDM, MIMO |
| IEEE 802.11ac | 2,4 nebo 5 | 1800 | OFDM, MIMO |

**Výhody** (7):

- Na rozdíl od paketových rádiových systémů, IEEE 802.11 využívá nelicencované rádiové pásmo a individuální uživatel nepotřebuje souhlas místních úřadů,
- umožňuje vybudovat LAN bez kabelů, a tak snížit náklady na vybudování či rozšiřování sítě. Bezdrátové sítě jsou výhodné v prostorách, kde nelze použít kabely např. v historických budovách,
- Wi-Fi produkty jsou na trhu široce dostupné. Rozličné značky přístupových bodů a klientských síťových adaptérů mezi sebou spolupracují na základní úrovni,
- konkurence mezi výrobci významně snížila ceny,
- více přístupových bodů a síťových adaptérů podporuje různé stupně kryptování, díky čemuž je komunikace zabezpečena před zachycením nechtěnou osobou.

**Nevýhody** (7):

- Použití Wi-Fi pásma 2,4 GHz ve většině zemí nevyžaduje licenci za předpokladu, že zůstane pod limitem 100 mW a akceptuje rušení z jiných zdrojů včetně rušení, které zapříčiní nefunkčnost zařízení,
- přidělené pásma a operační omezení nejsou na celém světě,
- standardy 802.11ba 802.11g používají nelicencované pásmo 2.4 GHz, které je přeplněné jinými zařízeními např. Bluetooth, mikrovlnné trouby, bezdrátové telefony nebo zařízení pro bezdrátový přenos video signálu. To může způsobit snížení výkonu,
- přístupové body se dají využít k ukradení osobních informací vysílaných Wi-Fi klienty,
- nezabezpečené přístupové body (nebo nesprávně nakonfigurováno přístupové body) může záškodník využít k anonymnímu útoku.

**IEEE 802.16**

Protiváhou bezdrátových systémů pro přenos dat provozovaných v bezlicenčních pásmech se staly bezdrátové sítě pracující v licencovaných pásmech. Jsou označovány

jako FWA (Fixed Wireless Access) a představují širokopásmové bezdrátové řešení lokálního přístupového okruhu. Označují se často jako Fixed Radio Wireless nebo Wireless in Local Loop. Původní řešení FWA používalo přenos v pásmu 26 GHz.

První norma pro bezdrátové metropolitní sítě IEEE 802.16 byla vyvinuta v roce 2001. Byla určená pro frekvence 10 až 66 GHz a při přenosu požadovala přímou viditelnost, tak se stala nepoužitelnou pro nasazení v praxi (7).

**WiMAX**

Jde o stále se vyvíjející bezdrátovou technologií, která je definována v řadě norem IEEE 802.16. Byla přijata v roce 2004 a umožňuje používat pásma v rozmezí 2 GHz až 11 GHz. Bez potřeby přímé viditelnosti má ve venkovských oblastech dosah 50 km a v husté zástavbě 3-5 km. Na rozdíl od jiných specifikací WiMax přenáší data v několika frekvenčních pásmech, díky čemuž minimalizuje možnost rušení s jinými rádiovými aplikacemi. V závislosti od volby spektra se mění i dosah a maximální rychlost přenosu. Používá modulaci OFDM, která nabízí možnost dosažení vysokých rychlostí přenosu dat ve ztížených podmínkách na vysílání či příjmu signálu. OFDM rozděluje širokopásmový signál do 256 úzkopásmových kanálů, z nichž každý přenáší asi 50 kb / s. Kanály jsou sice poměrně blízko ve frekvenčním pásmu, nedochází však k překrytí, a tak nehrozí jejich vzájemné rušení. Při přenosu pomocí OFDM také lze zanedbat možnost vzniku rušení způsobeného různými trasami šíření signálu či útlumu signálu ve venkovním prostředí (7).

**Bezpečnost bezdrátových sítí**

Bezdrátové sítě mají oproti kabelovým sítím jednu velkou nevýhodu z hlediska bezpečnosti. U bezdrátových sítí není technicky možné omezit prostor, ve kterém je možné signál zachytit. U kabelových sítí se musíme dostat ke kabelům, abychom byli schopni odposlouchávat komunikaci, ale u bezdrátových sítí nám stačí být jen v dosahu signálu vysílače, což v některých případech může být oblast i několik kilometrů od vysílače. Proto je nutné u těchto sítí zavést bezpečnostní opatření, které zabrání potencionálním útočníkům vniknout do sítě, nebo odposlouchávat data (8).

## 1.4 Model FCAPS dle normy ISO

Standardizaci síťového managementu vytvořila mezinárodní organizace ISO (International Standards Organization). Sestavila model FCAP, který se skládá z pěti částí - Fault (Problém), Configuration (Kongigurace), Accounting (Účtování), Performance (Výkon), Security (Bezpečnost).

Tento model odpovídá základním funkcím síťového managementu, jenž jsou popsány v dokumentu OSI Management Framework. Jde o čtvrtou část standardu OSI Basic Reference Model (ISO/IEC 7498-4) (9).


**Obr. č. 3: Model FCAP** (Zdroj: 10)

### 1.4.1 Správa výkonu

Efektivní správa sítě vyžaduje sledování krátkodobých a dlouhodobých výkonových statistik systému. Sebrané údaje zahrnující využití, chybovost, čas odezvy a dostupnost linky atd., jsou cenným nástrojem při identifikaci trendů v síti vzhledem k plánování kapacit sítě. Při znalosti těchto parametrů je možné reagovat dvěma způsoby (9):

**Reaktivní management** - při monitorování zvolených parametrů lze nastavit jejich prahové hodnoty, které nesmějí přesáhnout. Pokud však dojde k jejich překročení lze na

tuto událost reagovat předdefinovanou akcí např. zasláním varovné zprávy správci systému.

**Proaktivní management** - pomocí simulačních metod (které obsahují dnešní dokonalejší management aplikace) můžeme lépe plánovat potřebné změny a případný růst sítě a vliv těchto změn na výkonnost sítě. Jde především o metodu "what if", např. když provedu tuto topologickou změnu, jak to ovlivní zatížení tohoto segmentu atd.

### 1.4.2 Správa konfigurace

Zabývá se monitorováním sítě a její konfigurací. Tato oblast je zvláště důležitá, protože mnoho problémů vzniká jako přímý důsledek změn konfiguračních souborů, aktualizací softwaru nebo při změnách hardwaru. Konfigurační subsystém provádí zálohu veškerých konfiguračních informací do databáze pro další snadný přístup (11).

**Cílem správy konfigurace je** (11):

- Shromažďování a ukládání konfigurací ze síťových zařízení (lze provést vzdáleně nebo lokálně
- Zjednodušení konfigurace zařízení
- Sledování změn provedených v konfiguraci
- Plánování pro budoucí rozšíření

### 1.4.3 Účetní a evidenční správa

Slouží k monitorování využití sítě a aktivit jednotlivých entit komunikace (uživatel, skupina, počítač, síť, služba apod.) za účelem regulování sítě a fakturace za poskytnuté služby (11).

### 1.4.4 Správa poruch a chyb

Zabývá se detekcí a opravu chyb v síti, jde o nejpoužívanější oblast správy sítě, protože chyby a poruchy jsou vidět uživateli. Spravuje automatické řešení problémů na síti, tak aby síť fungovala efektivně pro každého účastníka v ní. Zdroje problémů dokáže izolovat a zajišťuje odeslání upozornění o jejich existenci odpovědným osobám, které mají za úkol jejich odstranění. Zabezpečuje sledování stavu daného problému i během jeho řešení a manažer je o stádiu jeho řešení dostatečně informován, protože chyby

mohou způsobit nečekanou degradaci kvality provozu celé sítě. Chybový management je implementován v největší míře ze všech funkčních oblastí modelu FCAP (11).

### 1.4.5 Správa bezpečnosti

Kontrola přístupu k hardwarovým komponentám sítě tak, aby nebyla síť sabotována a citlivé informace byly dostupné pouze pro autorizované uživatele. V pravidelných časových intervalech sbírá a analyzuje informace související s bezpečností a zaznamenává bezpečnostní narušení (11).

## 1.5 Management ICT služeb podle ITSM / ITIL

IT služby jsou služby, které poskytuje IT oddělení uživatelům a oddělením mimo IT. Uživateli služeb mohou být zaměstnanci, nebo celé oddělení firmy (interní uživatelé) nebo subjekty mimo organizaci (externí uživatelé), rozlišujeme: (12).

- **management IT infrastruktury**
- **management IT služeb** - řízení služeb, které poskytuje IT oddělení interním nebo externím uživatelům. Nezabývá se ani tak technickými, jak organizačně – řídicími záležitostmi.

### 1.5.1 ITSM (Information Technology Service Management)

Zahrnuje řízení informačních i komunikačních technologií. Obsahem ITSM je definování procesů, které by měly být implementovány v podniku za účelem zajištění nepřetržitého a kvalitního poskytování IT služeb při vynaložení optimálních nákladů (12).

**Řízení IT služeb se provádí s ohledem na odběratele** (12):

- ITSM je zákaznicky orientovaný, zákazník je ten, kdo službu odebírá a kdo za ni platí.
    - **Externí zákazník** - obchodní partner podniku, který si kupuje některý z podnikových produktů (výrobek nebo službu).
    - **Interní zákazník** - uživatel podnikové IT infrastruktury (tj. v zásadě vedoucí pracovník některého obchodně - provozního útvaru podniku.

- Poskytování IT služeb, které jsou skutečně požadované. Předpokladem je rozumět tomu, co je požadováno, tzn. rozumět podnikovým cílům, strategiím a znát obchodní procesy. Potřeba komunikace s odběratelem služeb a zapojit ho do všech aktivit souvisejících s poskytováním IT služeb (12).

- Neposkytovat služby, které nejsou požadovány. Veškeré náklady na služby (tzn. investice do IT infrastruktury) by měly být odsouhlasené odběrateli těchto služeb. Nerealizovat "vylepšení IT infrastruktury", které žádná z provozních složek podniku nepotřebuje (12).

- Poskytovat služby nákladově optimální, je třeba měřit náklady spojené s poskytováním každé služby, dále je třeba informovat odběratele služeb o nákladech spojených s jejich požadavky na odběr IT služeb. Odběratelé musí být informováni o tom, že (12):
    - kvalitnější služba nese vyšší náklady
    - závislost "náklady vs. kvalita " nebývá pro IT služby lineární, ale exponenciální

### 1.5.2 ITIL (Information Technology Infrastructure Library)

Vznikl jako soubor knižních publikací popisujících způsob řízení IT služeb a IT infrastruktury.

**V současnosti samostatný obor činnosti a podnikání, který zahrnuje** (12):

- Samostatnou knihovnu (v současnosti 5 publikací).
- Oblast vzdělávání a certifikace odborné způsobilosti.
- Oblast poskytování konzultačních služeb.
- Oblast vývoje a implementace softwarových nástrojů pro podporu ITSM procesů.
- Mezinárodní platformu profesionálů a odborné veřejnosti.

ITIL je rozsáhlý, konzistentní a procesně orientovaný rámec pro oblast IT Service managementu. Je založen na nejlepších zkušenostech z praxe ITSM (tzv. Best Practice), tzn., že: mnoho oblastí, které ITIL popisuje, nepředstavuje pro lidi z praxe zásadně nic

nového, nebo neznámého. Některé aktivity a principy, které jsou již v řadě podniků implementovány, mohou být zásadám a principům ITIL podobné. Zahrnuje tedy všechny zkušenosti z praxe do jednoho uceleného a konzistentního rámce. Dává všechny ITSM procesy do vzájemných souvislostí a zavádí jednotnou a používanou mezinárodní terminologii (12).

**Charakteristické rysy ITIL** (2):

**Procesní řízení -** Proces je logický sled úkolů transformujících nějaký vstup na nějaký výstup**.** Plnění jednotlivých úkolů v procesu je zajišťováno rolemi s jasně definovanými odpovědnostmi. Celý proces je řízen, monitorován, měřen, vyhodnocován a neustále vylepšován, což je odpovědnost vlastníka procesu.

**Zákaznicky orientovaný přístup -** Všechny procesy jsou navrhovány s ohledem na potřeby zákazníka. Každá aktivita a každý úkon v každém procesu musí přinést přidanou hodnotu pro zákazníka, pokud ne, tak je daná činnost zbytečná.

Jednoznačná terminologie umožňuje předcházet "nedorozuměním" způsobeným odlišným výkladem jednotlivých pojmů. Rámec ITSM procesů podle ITIL je nezávislý na jakékoliv platformě. Knihovna ITIL je volně přístupná, tj. každý si může ITIL knihy koupit a implementovat procesy ITSM podle ITIL.

**ITIL publikace - pět základních titulů** (12):

- **Service Strategy (strategie služeb)** - zahrnuje koncepty a doporučení ohledně strategie řízení služeb a plánování přínosů. Propojení byznys plánů se strategií IT služeb.
- **Service Design (návrh služby)** - zahrnuje koncepty návrhu služeb včetně návrhu architektury, procesů, pravidel, dokumentace a flexibility pro případ budoucích požadavků. Také se musí brát ohled na dimenzování rezerv, udržitelnost provozu služby, bezpečnost apod.
- **Service Transition (přechod služby)** - hovoří o implementační části samotného procesu. Zahrnuje procesy - plánování a podpory přechodu, management změn, management konfigurací a aktiv služby, management vydání a nasazení, validace a testování služby, ohodnocení změn, management znalostí.

- **Service Operation (provoz služby)** - zahrnuje poznatky pomocí, kterých se dosahuje dodávka služeb v dohodnuté kvalitě pro koncové uživatele. Zahrnuje procesy - management událostí, management incidentů, zpracování požadavků, management problémů, management přístupů.
- **Continual Service Improvement (nepřetržité zlepšování služeb)** - sestává z úpravy a přizpůsobování IT procesů měnícím se požadavkům.

**Event management (Management událostí)**

Event (událost) - jakákoliv detekovatelná událost, která má význam pro řízení IT infrastruktury nebo poskytování IT služby. Události jsou typicky oznámení generované IT službou, konfigurační událostí nebo monitorovacím nástrojem. Dále poskytuje schopnost detekovat události, určovat jejich smysl a určit vhodné řídící činnosti (12).

**Incident management (Management incidentů)**

Incident je neplánované přerušení služby IT nebo snížení kvality služby IT. Porucha konfiguračního prvku, která dosud neměla dopad na službu, je také incidentem. Incident Management je proces pro řešení všech incidentů, což může zahrnovat poruchy, dotazy nebo žádosti hlášené uživateli (obvykle prostřednictvím telefonního hovoru na technickou podporu), technickými pracovníky, nebo jsou detekovány automaticky a zaznamenány pomocí nástrojů pro monitorování událostí (12).

## 1.6 SNMP (Simple network management protocol)

SNMP je protokol aplikační vrstvy umožňující výměnu informací potřebných pro management sítě mezi síťovými zařízeními. Tento protokol je součástí řady protokolů TCP/IP (Transmission Control Protocol/Internet Protocol) a umožňuje administrátorům spravovat výkonnost sítě a především najít a řešit problémy, které v síti vznikly.

Existují 3 verze protokolu SNMP verze 1 (SNMPv1), verze 2 (SNMPv2) a verze 3 (SNMPv3). Verze mají mnoho společného, ale novější verze obsahuje vylepšení oproti předchozí verzi jako další operace tohoto protokolu (11).

### 1.6.1 Základní prvky SNMP

SNMP využívá koncepci manažer – agent, je typicky nasazováno na jednom či více správcovských počítačích (manažeři), jejichž úkolem je sledovat nebo řídit skupinu počítačů nebo jiných zařízení na síti. Na straně sledovaných zařízení je spuštěn agent, který následně poskytuje pomocí SNMP informace manažerovi. Data agentů jsou evidována jako proměnné. Protokol umožňuje jejich aktivní správu, kdy lze tyto proměnné vzdáleně modifikovat a změnit tak konfiguraci (11).

**Vlastnosti SNMP**

- Nelze měnit strukturu MIB přidáváním nebo mazáním instancí objektů,
- je možné vydávat příkazy k provedení určité činnosti,
- je možný přístup jen k objektům nacházejícím se v koncových uzlech registračního stromu,
- Je možné provádění operací nad dvojrozměrnými tabulkami.

**Tři aspekty řízení přístupu** (11):

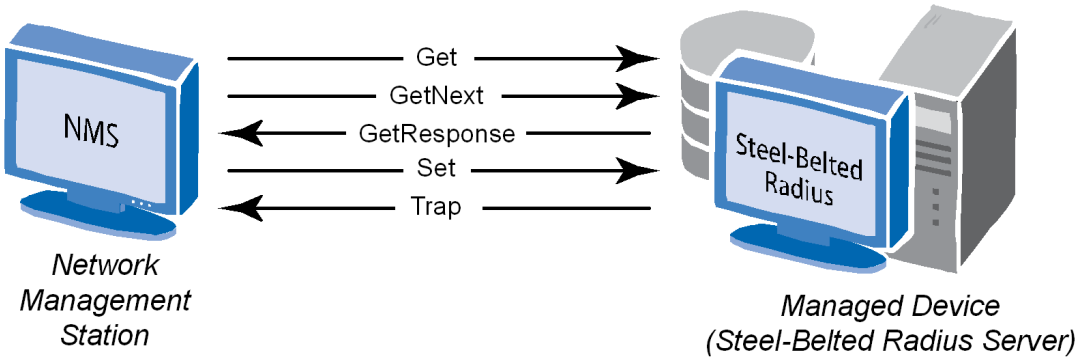
- **Autentifikace** - agent může omezit právo na přístup k MIB pouze pro autorizované stanice,
- **Přístupová politika** - agent může mít různá přístupová práva pro různé stanice,
- **Proxy služba** - agent může sloužit jako proxy pro další řízené stanice. Z toho vyplývá možnost provádění autentizace a přístupové politiky pro jiné řízené systémy v daném proxy systému.

### 1.6.2 SNMP zprávy

V SNMP jsou informace mezi řídící stanicí a agentem vyměňované ve formě SNMP zpráv (13):

- **GetRequest PDU** - slouží k získání hodnoty instance objektu od agenta, může obsahovat seznam více objektů, operace je atomická (pokud nemůže být zaslána jedna z požadovaných hodnot, tak nejsou zaslány žádné hodnoty).

- **GetNextRequest PDU** - slouží k získání hodnoty instance objektu, která nesleduje v lexikografickém pořadí za instancí uvedenou v zaslané zprávě. Může obsahovat seznam více objektů a operace je také atomická,
- **SetRequest PDU** - slouží ke změně hodnoty instance objektu u agenta. Musí obsahovat identifikátory instancí objektů a jim přiřazené hodnoty. Může obsahovat seznam více objektů a operace je také atomická. Zrušení hodnoty se provádí nastavením hodnoty na "invalid",
- **GetResponse PDU** - je vygenerován agentem, pouze pokud objekt obdrží příkaz GetRequest, GetNext nebo SetRequest,
- **Trap PDU** - slouží k zaslání nevyžádané zprávy agentem manažerovi, není potvrzován (3).




**Obr. č. 4: Zasílání SNMP zpráv** (Upraveno dle (12))

### 1.6.3 Vylepšení SNMPv2 a SNMPv3

**Oblasti, v nichž došlo k vylepšením ve SNMPv2** (11):

- **Struktura managementových informací** - Rozšířením makra definujícího typy objektů bylo přidáno několik nových datových typů. Změnilo se označování stávajících datových typů a byl přidán nový typ přístupu k objektům (read-create). Změnil se i způsob vytváření a rušení řádků v tabulce.

- **Protokolové operace** - byly přidány dva nové typy PDU
    - **GetBulkRequest PDU** - umožňuje minimalizovat počet protokolových výměn potřebných pro přenos velkého objemu managementových informací. GetBulkRequest pracuje na podobném principu jako

GetNextRequest, s tím, že umožňuje specifikovat počet lexikografických následovníků.

- **InformRequest PDU** - slouží pro výměnu informací mezi manažery.

Do SNMPv2 MIB byly přidány další informace týkající se konfigurace SNMPv2 manažera a agenta. U ostatních typů PDU (GetRequest, GetNextRequest) byla zrušena atomičnost (není atomická) → zasílá se chybová zpráva. SetRequest je atomická a rozdíl je v způsobu zpracování odpovědi a detailnějším popisu typu chyby v odpovědi. Trap má jiný formát (jako všechny SNMPv2 PDU kromě GetBulkRequest) a ostatní má stejné jako SNMP (9):

- **Spolupráce mezi manažery** - umožňuje výměnu informací mezi manažery. Definuje Manager-to-manager MIB, má dvě skupiny:
  - Alarm groupe,
  - Event groupe.
- **Bezpečnost** - snaha o vylepšení bezpečnosti

**Vylepšení ve SNMPv3**

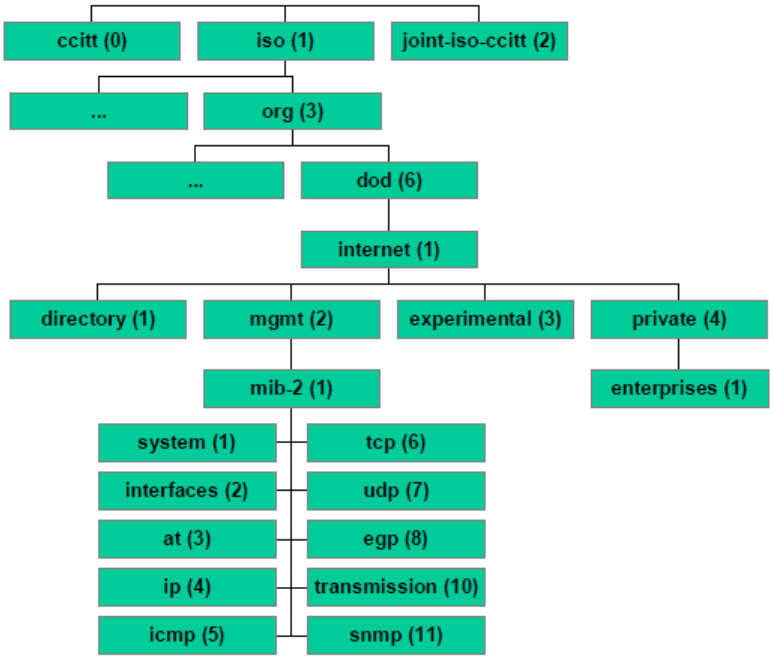
SNMPv3 není přímou náhradou za SNMPv1 nebo SNMPv2 ale jde o rozšíření SNMPv2 o bezpečnostní mechanismy. Dále umožňuje autorizaci (HMAC-MD5-96, HMAC-SHA-96) a kryptování přenášených zpráv (DES). Definuje novou architekturu agenta a manažera (každá SNMP entita sestává z modulů, které vzájemně spolupracují s cílem poskytovat managementové služby (9)).

### 1.6.4 MIB (Management information base)

MIB popisuje sadu objektů, které jsou předmětem správy. Sestává se z množiny řízených objektů a jejich atributů. Specifikace MIB je založena na objektově orientovaném principu, což umožňuje jednoduché přidávání nových tříd a funkcí pro řízené objekty. Specifikace nestanoví, aby MIB byla implementována pomocí objektově orientovaného databázového systému, nebo jinou objektově orientovanou technologií. Vyžaduje se, aby vyměňovaná informace mezi systémy v rámci protokolů managementu systémů (např. CMIP) dodržovala zásady objektově orientovaného návrhu (11).

**Řízený objekt je definován** (9):

- Atributy viditelnými na hranicích řízeného objektu.
- Operacemi, které mohou být s řízeným objektem prováděny.
- Chováním řízeného objektu jako odpověď na managementové operace.
- Oznámeními, která mohou být řízeným objektem generována.
- Podmíněnými balíky, které může řízený objekt obsahovat.
- Pozicí řízeného objektu ve stromu dědičnosti.




**Obr. č. 5: Struktura MIB** (Zdroj: 14)

Identifikátory objektů jsou posloupnosti čísel reprezentujících hierarchickou stromovou strukturu objektů v MIB. Stanice může procházet strukturou MIB a přistupovat k instancím objektů i bez znalosti struktury MIB a identifikátorů instancí objektů (9).

## 1.7 RMON (Remote Network Monitoring)

U standardu RMON došlo k rozšíření možností správy a k odlehčení komunikace přemístěním velké části činnosti na agenta. Základní myšlenkou při návrhu RMON byla potřeba mít inteligentního agenta, pro samostatné monitorování na straně spravovaného zařízení. RMON MIB standard umožňuje vzdáleně monitorovat Ethernet i Token Ring segmenty a to využitím již zavedeného protokolu SNMP (11):

### 1.7.1 Základní skupiny RMON MIB (11):

- **Statistic** - sleduje statistiku provozu na Ethernetovském segmentu,
- **History** - sbírá statistiky z celého segmentu sítě. Statistiky se nevztahují k jednotlivým stanicím připojeným k síti,
- **Alarms -** zpracování prahových hodnot,
- **Hosts** - záznam provozu aktivních zařízení v síti na základě IP nebo MAC adresy,
- **Hosts Top N -** uspořádané statistiky založené na MAC adresách, ty nejsou mimo segment LAN zachovány,
- **Matrix** - Strukturuje údaje podle párů MAC adres stanic, které navzájem komunikují,
- **Events -** události, které jsou zaznamenávány po překročení předem definovaných prahových hodnot,
- **Filters -** nastavení podmínek pro generování statistik,
- **Packet Capture** - odchytávání paketů a jejich přeposílání diagnostickému nástroji.

## 1.8 IP toky

Další metodou pro monitorování a analýzu sítě je monitorování síťových toků (flow monitoring). Základním pojmem a jednotkou, se kterou metoda pracuje je tzv. tok (flow) (9).

Tok je množina IP paketů procházejících přes pozorovací bod (observation point) v síti během určitého časového intervalu. Přičemž všechny pakety patřící danému toku mají množinu společných vlastností. Každá vlastnost je definována jako výsledek aplikování funkce na následující hodnoty (11):

1. **Jedna nebo více položek z hlavičky paketu (packet header) -** například cílová IP adresa z transportní hlavičky paketu (transport header) nebo cílový port z aplikační hlavičky paketu (application header).
2. **Jedna nebo více charakteristik paketu samotného** - například číslo MPLS návěstí (MPLS labels).

3. **Jedna nebo více položek odvozených od zpracování paketu**

Paket patří do daného toku, pokud splňuje všechny definované vlastnosti toku. Také je možné říci, že IP tok je jednosměrná posloupnost paketů stejného protokolového typu přenášených mezi stejným zdrojovým a cílovým místem během časové periody (11).

Proces monitorování toků produkuje záznamy o tocích (flow records). Záznam toku obsahuje informace o specifickém toku, který byl zachycen na pozorovacím bodě. V průběhu monitorování toků dochází k zachycení hlaviček paketu, označení časem (Timestamping), vzorkování (sampling), klasifikaci a udržování záznamů o tocích. Udržování paketů zahrnuje tvorbu nových záznamů, obnovu již existujících záznamů, výpočet statistických dat, vymazávání záznamů a prodávání toků exportnímu procesu (export process). Exportní proces následně předává záznamy toků kolektoru, kde běží proces sběru záznamů (collection process), který získané informace z toků filtruje a agreguje, dále pak tato data ukládá k následné případné analýze (15).

### 1.8.1 Využití monitorování IP toků

Metoda monitorování (měření) toků má různé výhody a možnosti uplatnění, hlavní výhodou je schopnost analyzovat a monitorovat rozsáhlé sítě při vysokých síťových rychlostech. Záznamy o tocích poskytují přesné statistické data o povaze sledované sítě. Důležité je však si uvědomit, že technologie pracuje (zjednodušeně řečeno) s údaji kdy, co, kde a kam teče sledovanou sítí. Tedy informace o stavu síťových zařízení, či dokonce možnosti přímé zprávy jsou mimo účel této technologie. Přesto účinnost sběru dat o tocích a možnosti následné analýzy těchto dat poskytují cenné informace v různých oblastech síťové infrastruktury (11).

- **Bezpečnost sítě, detekce útoku nebo zahlcení (Attack, intrusion detection)** – analýza toků hraje důležitou roli v ochraně sítě před vnějším napadením i detekcí vnitřní infiltrace. Pomocí sledování toků je možné detekovat nestandardní nebo neočekávané události v síti. Také následně poskytuje cenné informace o útočících tocích a pomáhá tak stanovit obrannou strategii. Pomocí analýzy toků se dají eliminovat hlavně DoS útoky a odhalovat stanice napadené viry (11).

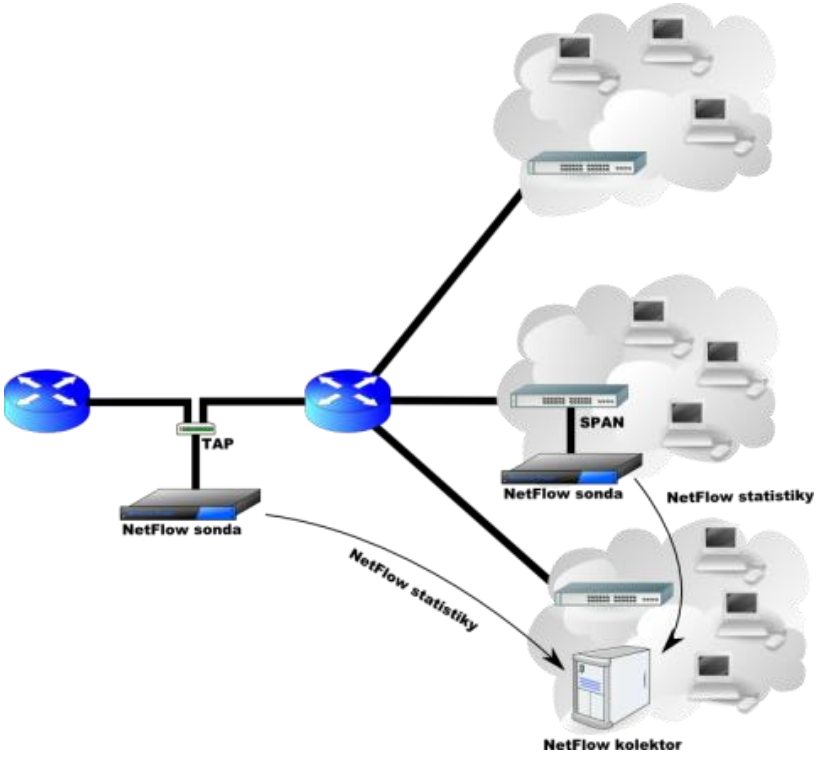
- **Profilování provozu (traffic profiling)** - je proces, který charakterizuje toky použitím definovaného modelu. Model reprezentuje vybrané sledované atributy toku, jako například délka trvání toku, protokol atd. Vytváří základní předpoklad pro plánování a rozšiřování sítě, analýzu trendů a další podobné aktivity. Záleží na cílech profilování provozu, které statistická data a s jakou přesností jsou sledována. Typicky potřebné informace k profilování jsou distribuce používaných služeb a protokolů, množství paketů specifického typu a nejčastější profil toku (11).
- **Plánování provozu (traffic engineering)** - cílem je optimalizovat zatížení síťových zdrojů a výkon směrování dat. Převážně se takto sleduje provoz v rámci autonomní sítě (AS). Analýza proudění toků v síti poskytuje informace o zatížení jednotlivých aktivních prvků sledováním množství proudících toků a tím pádem podává i cenné informace pro vyrovnání zátěže a možnosti použití jiných směrovacích cest (11).

### 1.8.2 NetFlow

Jedná se o otevřený protokol vyvinutý společností Cisco Systems, který byl původně určený jako doplňková služba k směrovačům Cisco. Hlavním úkolem je monitorovat síťový provoz na základě IP toků, který poskytuje jak administrátorům, tak i manažerům podrobný náhled do provozu na síti v reálném čase. Pro ISP je důležitý, že na základě NetFlow statistik mohou svým zákazníkům účtovat ceny služeb v závislosti na množství přenesených dat. S pomocí statistik je možné odhalovat vnější i vnitřní incidenty, úzká místa v síti, dominantní zdroje provozu, efektivněji plánovat budoucí rozvoj sítě, sledovat, kdo komunikoval s kým, jak dlouho a s pomocí kterého protokolu (13).

NetFlow architektura se obvykle skládá z několika exportérů a jednoho kolektoru. Exportér je pak připojen k monitorované lince a provádí analýzu procházejících paketů, na základě zachycených IP toků tak generuje NetFlow statistiky a ty exportuje na kolektor, což je zařízení s velkou úložnou kapacitou, které sbírá statistiky z většího počtu exportérů a následně je ukládá do databáze.

Tyto data následně vyhodnocuje aplikace, která je umí efektivně vizualizovat a generovat z nich přehledy v podobě grafů a tabulek (13).




**Obr. č. 6: NetFlow architektura** (Zdroj: 16)

## 1.9 SWOT analýza

SWOT analýza je základním nástrojem, který se používá k vyhodnocení současného stavu z různých hledisek, a to z hlediska silných a slabých stránek, příležitostí a ohrožení. Zároveň nastiňuje možné alternativy budoucího vývoje, možnosti na jejich využití, případně jejich řešení. Cílem analýzy je posouzení vnitřních předpokladů podniku k uskutečnění určitého podnikatelského záměru a podrobení rozboru i vnějších příležitostí a omezení určovány trhem.

V současnosti neexistuje žádná firma izolovaně od okolního světa. Nachází se uprostřed všeho dění a působí na ni mnoho negativních a pozitivních vlivů, ty které převažují, rozhodují o budoucnosti firmy. Záleží jen na tom, jak je na různé vlivy společnost připravena a jak se s nimi dokáže vypořádat. SWOT analýza hodnotí silné (strenghts), slabé (weaknesses) stránky společnosti, hrozby (threats) a příležitosti (opportunities) spojené s podnikatelským záměrem, projektem nebo strategií (17).

## 1.10 Lewinův model změn

Americký sociální psycholog Kurt Lewin vypracoval model, ve kterém je změna charakterizována jako stav nerovnováhy mezi hybnými silami (tlaky ve prospěch změny) a odporujícími silami (tlaky proti změně). Naopak změna nemůže nastat, pokud jsou síly v rovnováze (17).

Implementace představuje složitý proces plný změn. Změna je přechod z jedné základny či úrovně na jinou základnu nebo úroveň. Tento přechod se uskutečňuje postupně jako série organizačních, technologických, personálních nebo psychologických událostí. Má tedy charakter procesu. Lewin rozdělil proces změny do 3 základních fází (17):

- **rozmrazení,**
- **změna,**
- **opětovné zamrazení.**

Rozmrazení nastává tehdy, když se dospěje k poznání, že současný stav nevyhovuje. To znamená, že současná organizační struktura a technologie jsou neúčinné nebo dovednosti pracovníků či jejich postoje jsou nepřiměřené. Rozmrazení mimořádně stimuluje vznik krizí (17).

Změna se uskuteční jako reálný přechod podniku a jeho pracovníků do nového, adekvátnějšího stavu. Opětovné zamrazení nastává po realizaci změny, když nově rozvinuté chování, postoje nebo organizační struktury musí být stabilizovány, aby se staly trvalou součástí systému (17).

## 1.11 Matice RACI

Jedním z nejefektivnějších nástrojů na přiřazení odpovědností v rámci týmu je RACI matice (matice odpovědnosti). Identifikujte všechny funkce (aktivity, úkoly a rozhodnutí), které musí být provedeny pro efektivní fungování. Vyjasňuje úkoly a úroveň spoluúčasti na všech těchto funkcích pro každého člena týmu (17):

- **R - Responsible** - kdo je odpovědný za vykonání svěřeného úkolu,

- **A - Accountable** – kdo má absolutní odpovědnost, rozhoduje ano či ne a disponuje právem veta,
- **C - Consulted** - kdo může poskytnout cenou radu či konzultaci k úkolu,
- **I - Informed** – kdo musí být informováni po uskutečnění rozhodnutí,

# 2 Analýza současného stavu

Úvodem této kapitoly bude představena společnost CPU-Kocourek, s.r.o., která mimo jiné poskytuje bezdrátové internetové připojení v obci Babice nad Svitavou. Společnost požaduje výběr a implementaci vhodné technologie na základně provedené analýzy současného stavu a požadavků, které společnost definovala. Analýza současného stavu zahrnuje popis lokality, klientely, nabízeních tarifů, konkurence a analýzu informačních technologií.

## 2.1 Představení společnosti

| | |
|---|---|
| **Název** | CPU-Kocourek s.r.o. |
| **Sídlo** | Babice nad Svitavou 343, 66401 |
| **IČO \| DIČ** | 25599658 \| CZ25599658 |
| **Právní forma** | Společnost s ručením omezeným |
| **Předmět podnikání** | Výroba, obchod a služby neuvedené v přílohách 1 až 3 živnostenského zákona, výkon komunikační činnosti podle zákona č. 127/2005 Sb. o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích) |

Výběr a implementace technologie bude realizována pro společnost CPU-Kocourek s.r.o., která se zabývá tvorbou software, vývojem databází, poradenstvím v oblasti informačních technologií a od roku 2005 začala ve spolupráci se společností Q-net poskytovat bezdrátové internetové připojení a další datové služby v obci Babice nad Svitavou.

Od roku 2010 byla ukončena spolupráce se společností Q-net a byla vybudována nová vlastní síť pod názvem Net4Babice, ke které přestoupila většina dřívějších klientů.


**Obr. č. 7: Logo sítě NET4BABICE** (Zdroj: vlastní)

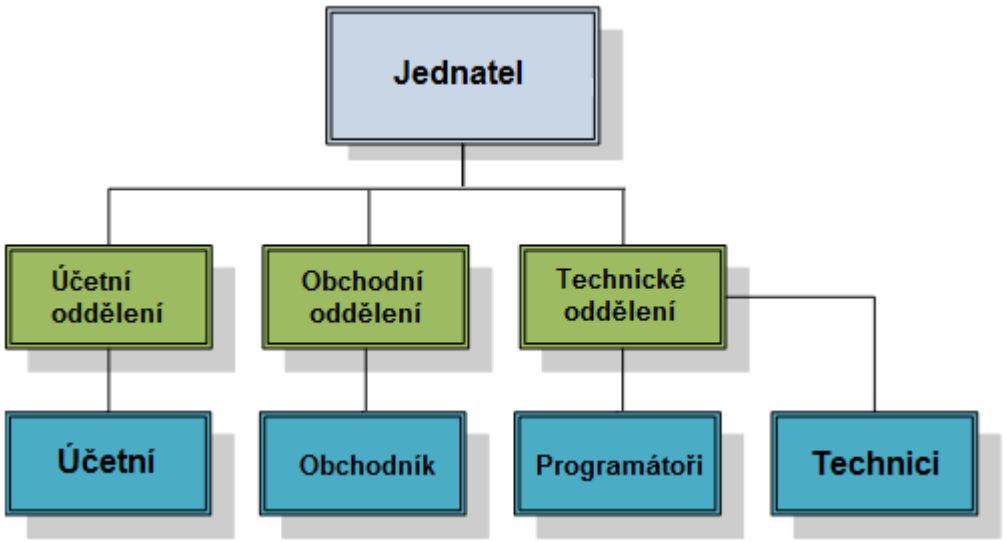
**Vize** - Udržení stabilního růstu společnosti, jenž dokáže konkurovat současným hlavním konkurentům v oblasti poskytování datových služeb a tvorbou software.

**Mise** - Udržet současné dobré vztahy s klienty a rozvíjet s nimi spolupráci. Navázat nové kontakty a rozšířit portfolio služeb a jejich kvalitu.

**Politika**

- Politiku společnosti vyhlašuje vedení společnosti v souladu s definovanými strategiemi společnosti.
- Pro vývoj vlastních řešení je využíváno nejnovějších technologií a znalostí.
- Přístup k zákazníkům se vždy vyznačuje především posouzením jejich potřeb a nalezením individuálního řešení.
- Se zákazníky se buduje oboustranně výhodný dlouhodobý vztah, který je založen na vzájemné důvěře a dobré zkušenosti.
- Všichni zaměstnanci společnosti se podílí na naplňování vizí a očekávání vlastníků a vedení společnosti.

### 2.1.1 Organizační struktura společnosti




**Obr. č. 8: Organizační struktura společnosti CPU-Kocourek s.r.o.** (Zdroj: vlastní)

Jednatelem a jediným vlastníkem společnosti CPU-Kocourek s.r.o. je pan Ing. Jaroslav Kocourek, ten rozhoduje o všech zásadních skutečnostech a jedná za společnost samostatně. Obchodní oddělení má zodpovědnost za komunikaci a celkovou obchodní

politiku s klíčovými zákazníky a plánuje marketingové akce. Technické oddělení soustřeďuje dostupné technické informace o provozu vlastní sítě, identifikuje možnosti zlepšování provozu, posuzuje jejich proveditelnost a koordinuje servisní a rozvojové činnosti. V současné době je zde zaměstnáno 12 pracovníků.

## 2.2 RACI matice

Přiřazení odpovědností členům týmu v projektech, procesech nebo jejich částech.

**Tab. č. 3: Raci matice** (Zdroj: vlastní)

| | Jednatel | Účetní | Programátor | Obchodník | Technik | Zákazník |
|---|---|---|---|---|---|---|
| **Tvorba IS** | I | | A | | | |
| **Monitoring** | I | | C | | A | C |
| **Datové služby** | I | | | C | R | C |
| **Účetnictví** | I | A | | | | |
| **Instalace** | A, I | | | | R | |
| **Marketing** | I | | C | A | | |

**R** – osoba odpovědná za vykonání úkolu **A** – osoba odpovědná za úkol jako celek

**C** – konzultant **I** – osoba, kterou je potřeba informovat

## 2.3 Analýza přístupové sítě

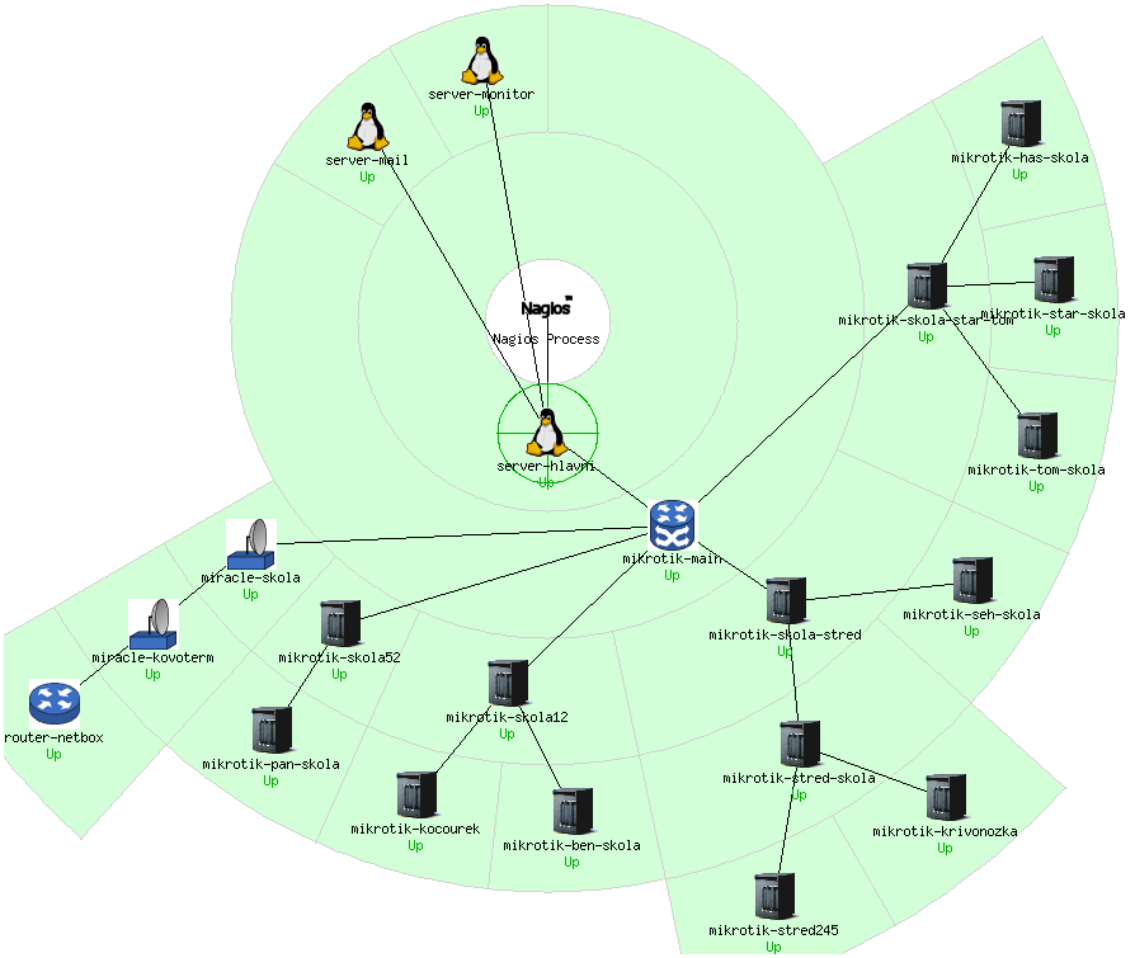
Připojení zákazníků do sítě poskytovatele je realizováno s využitím bezdrátových technologií v pásmu 5 GHz. Je zde vybudovaná široká síť přístupových bodů, která pokrývá téměř celou obec Babice nad Svitavou.

Používány jsou především produkty od následujících výrobců:

- MikroTik
- Miracle
- TP-Link
- Ubiquiti Networks
- Cisco

### 2.3.1 Mapa přístupové sítě

Na následujícím obrázku je znázorněna síťová mapa všech aktivních zařízení v síti mimo koncové klienty.




**Obr. č. 9: Mapa sítě** (Zdroj: vlastní)

### 2.3.2 Páteřní spoj Brno – Babice nad Svitavou

Základním předpokladem pro výkonnou a stabilní bezdrátovou síť bylo vybudování kvalitního páteřního spoje mezi obcí Babice nad Svitavou a Brnem, pro jeho realizaci společnost použila radiovou jednotku ORCAVE 1S10LA, která pracuje v pásmu 10 GHz. Venkovní jednotka má 2 Gigabitové Ethernet porty podporující napájení po Ethernetu. Management jednotky je In-Band a jednotka se ovládá přes webové rozhraní, každá strana spoje může mít stejné nebo odlišné průměry antén a stejné nebo odlišné

licence na přenosovou rychlost. Konektivita z Brna je poskytována společností SMART Comp, a.s. V případě výpadku hlavního spoje se automaticky aktivuje záložní spoj, který však nedisponuje takovou kvalitou. Během roku 2015 je plánovaná výměna tohoto spoje za modernější s vyšší přenosovou kapacitou.


**Obr. č. 10: Páteřní spoj z lokality Brno-Lesná** (Zdroj: vlastní)

### 2.3.3 Přístupové body

Přístupové body jsou realizovány za použití zařízení MIKROTIK RB433, který obsahuje 3x LAN port a 3x miniPCI sloty, nejčastěji je osazován kartami MikroTik R52H miniPCI.

### 2.3.4 Páteřní spoje v obci Babice nad Svitavou

V rámci modernizace sítě byly loni v létě veškeré páteřní spoje nahrazeny zařízeními UBIQUITI PowerBeam M5 400 AirMAX, jedná se o venkovní jednotku s 25 dBi MIMO anténou pracující v pásmu 5GHz s umožňuje přenosovou rychlost až do 150 Mb/s. PowerBeam je přímou náhradou jednotek NanoBridge M5 25 dBi a využívá novou konstrukci antény pro větší odolnost proti rušení, má lepší návrh pro snadnou

instalaci a je vybaven gigabit ethernetem. Předešlé páteřní spoje zůstaly zachovány a mohou sloužit jako záložní spoje, pokud dojde k výpadku.

**Obr. č. 11: UBIQUITI PowerBeam M5 400 AirMAX** (Zdroj: 18)

**Tab. č. 4: Specifikace produktu PowerBeam M5 400 AirMAX** (Zdroj: 18)

| | |
|---|---|
| **Operační mód/OS** | AP, Client, WDS/AirOS V |
| **Frekvence (GHz)** | 5 |
| **Normy** | 802.11a/n |
| **Chipset** | Atheros |
| **Max. výstupní výkon (dBm)** | 25 |
| **Citlivost (dBm)** | -96 |
| **Modulace** | OFDM, QAM |
| **Šifrování** | WPA-AES, WPA2-AES |
| **LAN port** | 1x RJ45 10/100/1000 Mbps |
| **Polarizace** | Horizontální a vertikální |
| **Procesor** | Atheros MIPS 24KC, 400MHz |
| **RAM (MB)/NAND (MB)** | 32/8 |
| **Napájení (V)** | 24V, 0.5A GigE PoE |
| **Provozní teplota min/max (°C)** | -40/70 |

### 2.3.5 Server

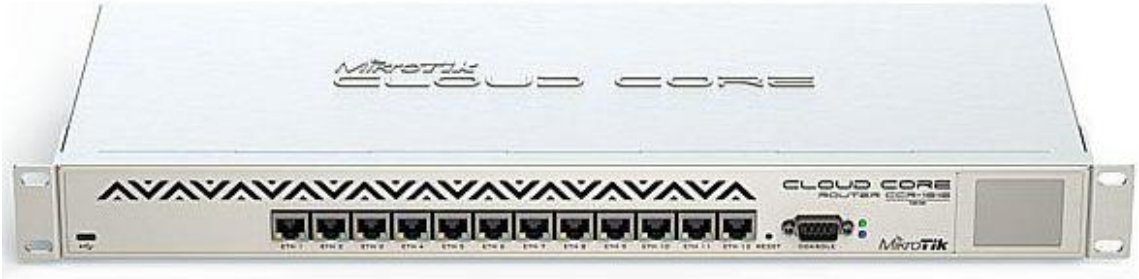
Jak již bylo zmíněno dříve, aktuálně je monitorován datový tok pomocí nástroje Cacti a je využívána správa pomocí programu AirControl. Oba nástroje běží na starším serveru Primergy Fujitsu Siemens RX100 S2, který je umístěn v hlavním racku na půdě základní školy.

**Specifikace serveru:**

- Provedení serveru je Rack 1U
- Intel Pentium 4 3.4 GHz
- 4GB (2x2GB) paměti DDR SDRAM - ECC s frekvencí 400MHz
- 2x 320GB disky SATA s rychlostí 7 200 otáček za minutu
- OS Linux
- Připojení k síti je zajišťuje dvojice Gigabitových portů.

### 2.3.6 Router

O řízení provozu se stará router MikroTik CCR1016-12G, který je vybaven 16-ti jádrovým procesorem Tilera Tile-Gx16 CPU s frekvencí 1.2 Ghz pro každé z jader. Má dva SODIMM sloty, standardně osazené 2GB RAM, které lze bez problémů rozšířit. Na zařízení běží propracovaný operační systém RouterOS L6. Router je vybaven dvanácti porty 10/100/1000 Mbit/s Gigabit Ethernet s funkcí Auto-MDI/X.




**Obr. č. 12: MikroTik CCR1016-12G** (Zdroj: 19)

Na půdě základní školy je umístěn uzamykatelný rack pro umístění potřebné technologie.

### 2.3.7 Klientská zařízení

Jako koncové zařízení pro příjem signálu jsou využívány pouze zařízení od společnosti Ubiquiti Networks. V současné době se využívá NanoStation M5 Loco AirMAX MIMO, jedná se o výkonnou venkovní jednotka včetně a integrované MIMO 2×2 13dBi antény. Jednotka umožňuje komunikaci reálnou rychlostí až 150 Mbps. Oproti

předchůdci NanoStation5 má silnější procesor taktovaný na 400 MHz,větší paměť a velmi jednoduchou a přehlednou administraci.

**Obr. č. 13: NanoStation M5 Loco AirMAX** (Zdroj: 18)

**Tab. č. 5: Specifikace produktu NanoStation M5 Loco AirMAX** (Zdroj: 18)

| | |
|---|---|
| **Operační mód/OS** | AP, Client, WDS/AirOS V |
| **Frekvence (GHz)** | 5 |
| **Normy** | 802.11a/n |
| **Chipset** | Atheros |
| **Max. výstupní výkon (dBm)** | 23 |
| **Citlivost (dBm)** | -96 |
| **Modulace** | OFDM, DBPSK, DQPSK, CCK, 64QAM, |
| **Šifrování** | WPA-AES, WPA2-AES |
| **LAN port** | 1x RJ45 10/100 Mbps |
| **Polarizace** | Horizontální a vertikální |
| **Procesor** | Atheros MIPS 24KC, 400MHz |
| **RAM (MB)/NAND (MB)** | 32/8 |
| **Napájení (V)** | 15/24 |
| **Provozní teplota min/max (°C)** | -30/80 |

## 2.4 Prostředky pro management

### 2.4.1 Informační systém

Společnost využívá svůj vlastní informační systém pro správu zákazníků. Každý zákazník má svůj soukromý přístup ke svému profilu, kde má kompletní přehled o službách, které využívá a snadno může provádět nejrůznější změny v osobních údajích, měnit poskytované služby (např. výši tarifu pro poskytování datových služeb), má přehled o uskutečněných platbách apod.

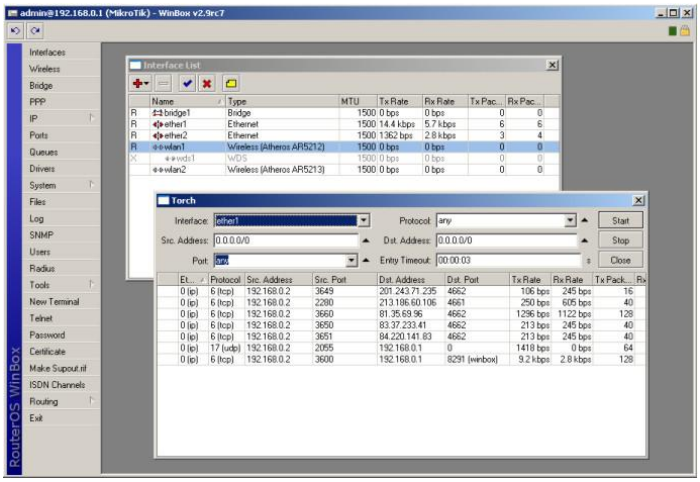
**Podpora procesů ze strany IS:**

- Zrychlení komunikace, sdílení znalostí
- Centralizace - vše na jednom místě
- Daňová evidence i podvojné účetnictví, fakturace, objednávky, mzdy, majetek
- Jednoznačnost – přiřazení zodpovědnosti
- Evidence a kontakt s klienty, hromadné oslovení
- Sdílení souborů řešení interních problémů

### 2.4.2 Software

Společnost využívá celou řadu nejrůznějšího software. Na pracovních stanicích je nejběžnější Microsoft Windows 7 na serverech pak Linux nebo Microsoft Windows Server 2008.

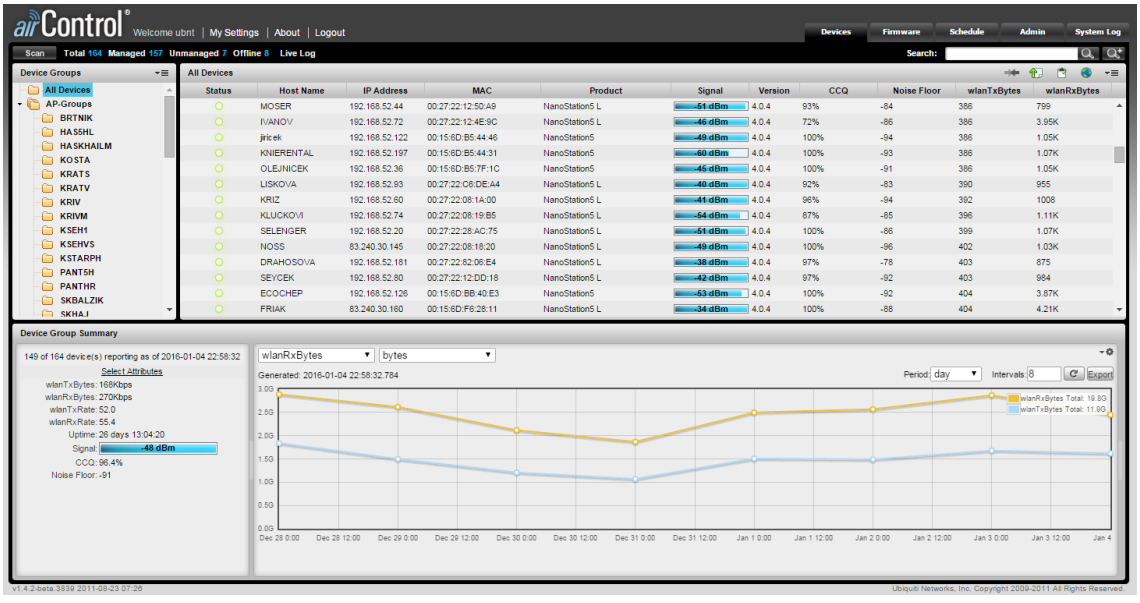
V oblasti poskytování datových služeb se používá celá řada software pro správu a nastavení sítě, většina z nich je volně k dispozici od výrobců aktivních prvků, které firma na své síti nasazuje. Pro bezdrátové páteřní spoje se využívá MirkoTik RouterOS, jedná se o routerový operační systém založený Linuxu. Komunikace s tímto OS se v současnosti provádí především přes GUI Winbox.



**Obr. č. 14: Náhled do uživatelského prostředí programu WinBox** (Zdroj: vlastní)

Dále je využíván nástroj Cacti, který je určen pro tvoření grafů síťového provozu. Jeho výhodou je přehledné webové GUI, pluginy, šablony a otevřenost pro vlastní získávání dat a tvorbu svých grafů a přehledů.

Mezi nejpoužívanější patří AirControl, což je aplikace pro správu sítě, která umožňuje správcům centrálně spravovat veškerá zařízení od společnosti Ubiqutii. Grafické prostředí je znázorněno na následujícím obrázku:



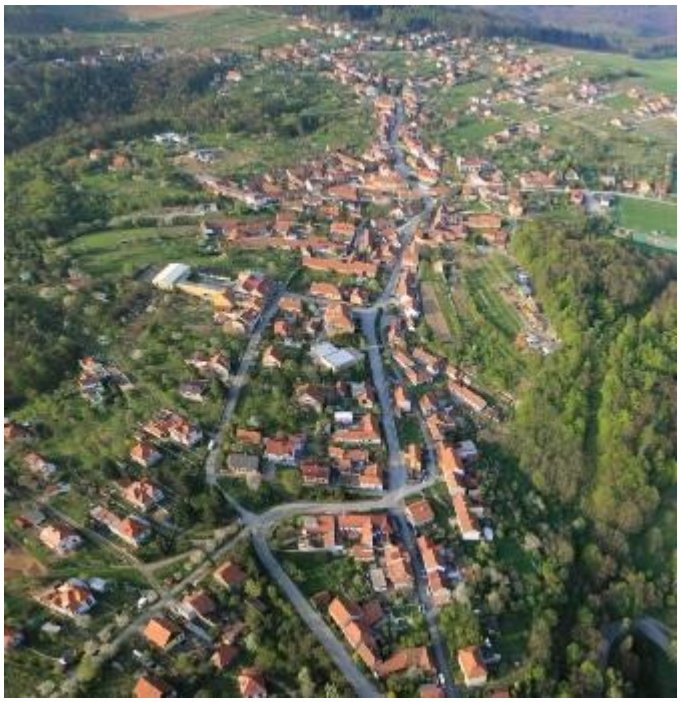
**Obr. č. 15: Náhled do webového rozhraní aplikace AirControl (**Zdroj: vlastní)

Společnost dále využívá systém RT (Request Tracker) pro sledování a správu vzniklých požadavků.

## 2.5 Analýza prostředí

### 2.5.1 Lokalita

Obec Babice nad Svitavou se nachází v Jihomoravském kraji přibližně 18 km severovýchodně od města Brna. Rozkládá se na území 17,42 $km^2$ v Drahanské vrchovině v nadmořské výšce 460 m n.m., v současné době zde žije 1068 obyvatel. V obci se nachází obecní úřad, farní kostel sv. Jana Křtitele, základní a mateřská škola, hasičská zbrojnice, sportovní hala a fotbalové hřiště TJ Sokol, knihovna, samoobsluha, soukromé stáje a dvě hospody.



**Obr. č. 16: Letecký snímek obce z roku 2012** (Zdroj: 20)

Pro poskytovatele internetového připojení je však nejdůležitější počet domů, jakožto počet potencionálních klientů, kterým může nabízet své služby. Dle informací z obecního úřadu je v obci aktuálně 347 trvale obydlených domů. Největší komplikací je pro poskytovatele terasovitý stoupající terén a celkové rozložení obce, pro pokrytí celé obce je potřeba rozsáhlá síť přístupových bodů. Výhodu však nese přímá viditelnost na město Brno, která je důležitá pro realizaci bezdrátového páteřního spoje a tím přivedení konektivity do obce. V obci probíhá developerský projekt Haas Fertigbau, který připravuje pozemky pro výstavbu 54 rodinných domů. Po domluvě s developerem

byly společně s výstavbou inženýrských sítí položeny mikrotrubičky pro zafukování optických kabelů.

### 2.5.2 Klienti

Počet připojených klientů do sítě NET4BABICE je v současné době 176. Většinu klientely tvoří domácnosti, kde připojení využívá několik členů rodiny na běžnou činnost na internetu (emaily, sociální sítě, sledování videa apod.). Připojení je také poskytováno několika podnikatelským subjektům, které v obci působí. Jejich připojení je řešeno individuálně dle jejich potřeb a požadavků (např. vlastním spojem a vyšší přenosovou rychlostí).

Společnost spolupracuje s obcí a využívá její budovy pro umístění svých zařízení a jako protislužbu poskytuje připojení k internetu zdarma ve všech obecních objektech (obecní úřad, škola, školka, zdravotní středisko, hasičská zbrojnice, knihovna).

Klienti si poskytovatele spojili obecně s IT a obrací se na něj i s jinými problémy než které by se týkaly poskytování datových služeb.

### 2.5.3 Nabízené tarify

Společnost nabízí svým i novým klientům tarify uvedené v následující tabulce. Není zde žádné omezení na přenášená data a v případě zájmu klienta je k dispozici i veřejná IP adresa zdarma.

**Tab. č. 6: Nabízené tarify platné k 1.1.2015 (**Zdroj: vlastní)

| Název služby | Rychlost stahování | Rychlost odesílání | Měsíční paušál |
|---|---|---|---|
| **Classic** | 16 Mb/s | 8 Mb/s | 400 Kč |
| **Speed** | 30 Mb/s | 15 Mb/s | 500 Kč |
| **Veřejná IP** | - | - | Zdarma |

Pro nové klienty jsou první tři měsíce zdarma, instalace a zapůjčení přijímače jsou také bez poplatku. Odstoupení od smlouvy je možné 2 měsíce po oznámení ukončení smlouvy.

## 2.6 Obchodní situace firmy

### 2.6.1 Trhy

Společnost se pohybuje na trhu statků a služeb. Své služby nabízí již od roku 2005. Za tuto dobu si vypracovala celou řadu stálých zákazníků, ke kterým se stále přidávají další, hlavně v oblasti datových služeb. Společnost se neustále snaží rozšiřovat nabídku poskytovaných služeb, ale začala upouštět od prodeje HW, protože zde je velice silná konkurence.

### 2.6.2 Konkurence

Konkurence v oblasti poskytování datových služeb je dnes poměrně značná, ale to se týká spíše větších měst. V obcích většinou vládne ten, kdo jako první začal nabízet své služby, pokud je jejich kvalita alespoň na standardní úrovni.

Společnost CPU-Kocourek s.r.o. má v obci Babice nad Svitavou nejlepší pokrytí bezdrátovým signálem, používá kvalitní zařízení a má rychlý servis při zjištění vzniklých poruch, proto její služby využívá téměř polovina obce. Mezi konkurenty patří - TS-Hydro, Maxtron a RYWASOFT. Následuje seznámení s konkurencí, které je vytvořeno z dostupných informací na webových stránkách poskytovatelů. V obci Babice nad Svitavou není dostupné ADSL připojení, a využití připojení prostřednictvím mobilních operátorů je v současné době velice pomalé a téměř nepoužitelné.

- **TS-Hydro**

Společnost začala poskytovat služby ve vedlejší obci Kanice od roku 2003, své působení rozšířila v obci Babice nad Svitavou v roce 2007 a to především v horní části obce. V roce 2014 společnost zprovoznila linku o rychlosti 200/200 Mb/s, která je připojena na mezinárodní páteřní optickou síť v Brně (21).

**Tab. č. 7: Nabízené tarify TS-Hydro platné k 1.1.2015** (Zdroj: 21)

| Název služby | Rychlost stahování | Rychlost odesílání | Měsíční paušál |
|---|---|---|---|
| Internet mini | 8 Mb/s | 1 Mb/s | 330 Kč |
| Speed | 30 Mb/s | 15 Mb/s | 480 Kč |
| Veřejná IP | - | - | 100 Kč |

Při připojení zákazník neplatí žádné aktivační poplatky, nastavení a instalaci, ale platí cenu instalovaného hardware.

- **Maxtron, s.r.o.**

Počátkem roku 2004 společnost vstoupila na pole rychle se rozvíjejícího oboru telekomunikačních služeb a zahájila poskytování připojení k internetu prostřednictvím bezdrátových technologií v obci Moravany. V průběhu roku 2005 byla zahájena expanze do okolních obcí a společnost začala poskytovat služby v jižní části Brna a přilehlých obcí. Trend rozšiřování pokrytí pokračoval i v následujících letech a pokračuje i v současnosti, kdy se firma chystá expandovat i do dalších lokalit. Tarify určené pro bezdrátové internetové připojení Babice nad Svitavou jsou následující (22):

**Tab. č. 8: Nabízené tarify Maxtron platné k 1.1.2015** (Zdroj: 22)

| Název služby | Rychlost stahování | Rychlost odesílání | Měsíční paušál |
|---|---|---|---|
| **Sprint 10** | 10 Mb/s | 3 Mb/s | 363 Kč |
| **Sprint 15** | 15 Mb/s | 3 Mb/s | 484 Kč |
| **Sprint 20** | 20 Mb/s | 3 Mb/s | 605 Kč |
| **Sprint 25** | 25 Mb/s | 3 Mb/s | 847 Kč |
| **Veřejná IP** | - | - | neuvádí |

- **RYWASOFT**

Poskytovatel telefonních a internetových služeb v Brně a okolí, dále zajišťuje správu sítí, softwarový a bezpečností audit. Při uzavření smlouvy na 12, 24 nebo 36 měsíců poskytuje akční ceny. Nabízené tarify pro bezdrátové připojení jsou následující:

**Tab. č. 9: Nabízené tarify RYWASOFT platné k 1.1.2015** (Zdroj: 23)

| Služba | Rychlost stahování | Rychlost odesílání | Cena | Akční cena |
|---|---|---|---|---|
| **1** | 3 Mb/s | 2 Mb/s | 299 Kč | 150 Kč |
| **2** | 15 Mb/s | 4 Mb/s | 482 Kč | 240 Kč |
| **3** | 20 Mb/s | 5 Mb/s | 599 Kč | 349 Kč |
| **Veřejná IP** | - | - | | neuvádí |

## 2.7 SWOT analýza

**Silné stránky**

- zkušený tým pracovníků s velkými zkušenostmi z oboru,
- vybudovaná základna zákazníků,
- dobrá pověst,
- dobře odváděná práce,
- využívání kvalitního kabelážního systému a výkonných aktivních prvků v síti,
- zájem zaměstnanců o další vzdělávání v oboru,

**Slabé stránky**

- malá společnost, která není příliš známá,
- nedostatečný monitoring sítě, rychlost reakce na vzniklé problémy
- nízké investice do reklamy - ani v místě podnikání, ani na internetu není o této společnosti moc slyšet,
- působení v malé oblasti.

**Příležitosti**

- technologické změny (např. optické kabely, nové pásma pro poskytování datových služeb)
- sledování konkurence a vývoj na trhu,
- nasazení nových moderních systému pro správu, monitoring apod.
- neustálé zvyšování úrovně poskytovaných služeb

**Hrozby**

- bezbariérový vstup nových firem do odvětví,
- pozdní reakce na technologické změny,
- někteří pracovníci jsou obtížně nahraditelní,
- možné zpoplatnění volných pásem k šíření bezdrátového připojení
- nižší cena konkurence, pro hodně zákazníků je rozhodující právě konečná cena za poskytované služby.

## 2.8 Hodnocení podnikání firmy z více pohledů

**Ekologické hledisko**

Společnost poskytuje bezdrátové datové služby, tudíž vytváří prostředí zamořené elektromagnetickým vlněním (takzvaným elektronickým smogem). Řada odborníků zkoumá, zda je toto prostředí zdraví škodlivé, ale ještě není natolik prozkoumané, aby bylo možné vynášet jednoznačné soudy o jeho škodlivosti či naopak nezávadnosti.

**Etické hledisko**

Zaměstnanci společnosti jsou příjemní lidé, kteří umí slušně vystupovat a jednat se zákazníky a problémy se snaží řešit v souladu s dobrými mravy.

**Legislativní hledisko**

Z tohoto hlediska musí společnost dodržovat předpisy a opatření vydané Českým telekomunikačním úřadem a hlavně se řídit zákonem č. 127/2005 Sb., o elektronických komunikacích. Veškerý software, který společnost využívá pro svoje účely, je legální nebo je jeho užívání freeware, tj. forma distribuce, která ponechává autorovi autorská práva, ale volně zpřístupňuje plně funkční software ostatním bez poplatků.

## 2.9 Problémy při běžném provozu

Společnost se nezabývá výrobou, proto nemusí řešit problémy s dovozem a uskladněním materiálu, ale musí zajistit dostupnost svých služeb 24 hodin denně a 7 dní v týdnu. Ovšem 100% spolehlivost zajistit nelze, protože může dojít k nějaké neočekávané poruše nebo výpadku. Příčinou může být chyba technika, porucha zařízení, delší výpadek elektřiny, ale servery a další důležitá zařízení jsou zálohována UPS, tak k výpadkům dochází minimálně. Vedoucí technického oddělení tvrdí, že největší problém jsou jarní bouřky, protože elektrické výboje způsobují škody na vysílačích a venkovní kabeláži. Používáním kvalitních prvků a správnou instalací zařízení se dá alespoň částečně těmto událostem předcházet.

Společnost se dále setkává s problémem neplatičů, hodně klientů neplatí za využívané služby včas. Nejprve obdrží upomínku o neuhrazení platby, ale většinou zaplatí, až jsou jim tyto služby zablokovány. Dost často se ozývají klienti, že jim něco nefunguje nebo

že mají pomalé připojení a v hodně případech je chyba na jejich straně a žádají o zcela zbytečný servis. Mezi nejčastější důvody patří povytažený kabel z počítače, špatně zapojený router po předchozí manipulaci (např. při malování, přesouvání nábytku), využívání torrentu, zavirovaný počítač apod.

Někteří pracovníci ve společnosti jsou jen obtížně nahraditelní, protože v něčem mají mnohem větší přehled než ostatní, a proto když někdo takový třeba onemocní nebo odjede na dovolenou, je velice náročné jej spolehlivě zastoupit.

## 2.10 Definice potřeb poskytovatele

Na základě provedené analýzy a konzultací s vedoucím technického oddělení byly definovány potřeby kladené na nově nasazovanou technologii. Bylo zjištěno, že největším nedostatkem managementu počítačové sítě je aktuálně správa chyb – monitoring. Definovány byly následující potřeby:

1. sledování všech klíčových komponenty IT infrastruktury,
2. posílání zprávy v případě, že kritický komponent selhal, nevykazuje požadované parametry, obnovil svou činnost apod. a to buď pomocí e - mailu, SMS nebo spuštěním skriptu, realizujícího předdefinované úkony,
3. generování reportů poskytující historická data a na základě kterých je možné přijímat rozhodnutí směřující k optimalizaci IT infrastruktury,
4. grafické zobrazování trendů a reporty využití kapacit umožňují identifikovat potřebné změny infrastruktury dříve, než přijde k problémům s jejich poddimenzováním,
5. Upřednostnění open-source řešení pro minimalizaci nákladů,
6. Aktivní vývoj a dostupnost dokumentace

## 2.11 Dostupná řešení vhodná pro management přístupové sítě ISP

### 2.11.1 Nagios

Tento projekt měl původně název Netsaint, v roce 2002 byl ale přejmenován na Nagios. Jedná se o open source monitorovací nástroj, navržený na okamžitou notifikaci

administrátora o problémech se sítí. Většinou je tak učiněno ještě před tím, než to pocítí koncoví uživatelé (24).

Nagios je určen pro běh v OS Linux a různých variantách OS Unix. Monitorovací služba spouští nespojité kontroly specifikovaných koncových stanic a služeb, použitím externích modulů, které vracejí výsledky kontrol hlavnímu modulu Nagios. Pokud jsou zjištěny problémy, služba je schopna poslat upozornění na předdefinované kontakty pomocí různých typů komunikace (email, SMS, nebo tzv.. Rychlá pošta - ICQ). Aktuální stav, historické záznamy a reporty jsou přístupné přes webové rozhraní (24).


**Obr. č. 17: Logo Nagios Core** (Zdroj: 24)

**Možnosti systému Nagios** (13):

- Možnost posílání notifikací do různých skupin podle zařízení a druhu problému,
- Podpora pro redundantní služby a monitorovací stanice,
- Monitoring síťových služeb (SMTP, POP3, http, NNTP, PING, atd..),
- Monitoring zdrojů vybraných stanic (zatížení procesoru, využití diskové kapacity a operační paměti, běžící procesy, atd..),
- Webové rozhraní pro prohlížení aktuálního stavu sítě, historie problémů a upozornění, záznamů, atd.,
- Jednoduchý autorizační návrh, který umožňuje specifikovat, kteří uživatelé budou mít přístup k zobrazení definované informace,
- Automatické generování historie stavu hosta / služeb,
- Komunikace mezi více operátory,
- Plánovat infrastrukturní upgrady dříve, než začnou způsobovat problémy,
- Reagovat na problémy už při jejich prvních příznacích,
- Automaticky odstraňovat detekované problémy,
- Koordinovat práci technických týmů na řešení obtíží

- Zajistit plnění podmínek stanovených v SLA,
- Minimalizovat náklady na provoz IT infrastruktury.

**Terminologie** (13):

- **Host** - zařízení, které chceme monitorovat. Obvykle počítač, server, switch, tiskárna apod.)
- **Host group** - skupina hostů stejného typu. Např. **servers** pro servery, **printers** pro tiskárny. Při jejich použití lze snadno všem hostům ve skupině definovat určité chování.
- **Serivce** - služba, kterou chceme na daném zařízení monitorovat. Buď jsou to služby veřejně dostupné (ping, HTTP, FTP) nebo lze za využití agentů sledovat údaje o volném místě na discích apod.
- **Service group** - skupina služeb. Stejně jako pro skupinu hostů existuje i skupina služeb, která zjednodušuje konfiguraci a zpřehledňuje reporting.
- **Contact a contact group** - kontakt a skupina kontaktů, kteří budou informováni, pokud dojde k nějaké kritické situaci.
- **Time period** - časový interval, ve kterém má být kontakt nebo skupina kontaktů informována o vzniklém problému.
- **Z hlediska architektury je možné Nagios rozdělit na tyto části** – démon, plugin, webové rozhraní, konfigurační soubory a stavová databáze.

**Pluginy**

Systém Nagios sám o sobě v podstatě nic neumí, než jen rozpoznat změnu stavu něčeho. Vlastní způsob zjištění stavu něčeho zajišťuje plugin, který Nagiosu vrátí stav. Nagios, získané odpovědi shromažďuje a vyhodnocuje (13).

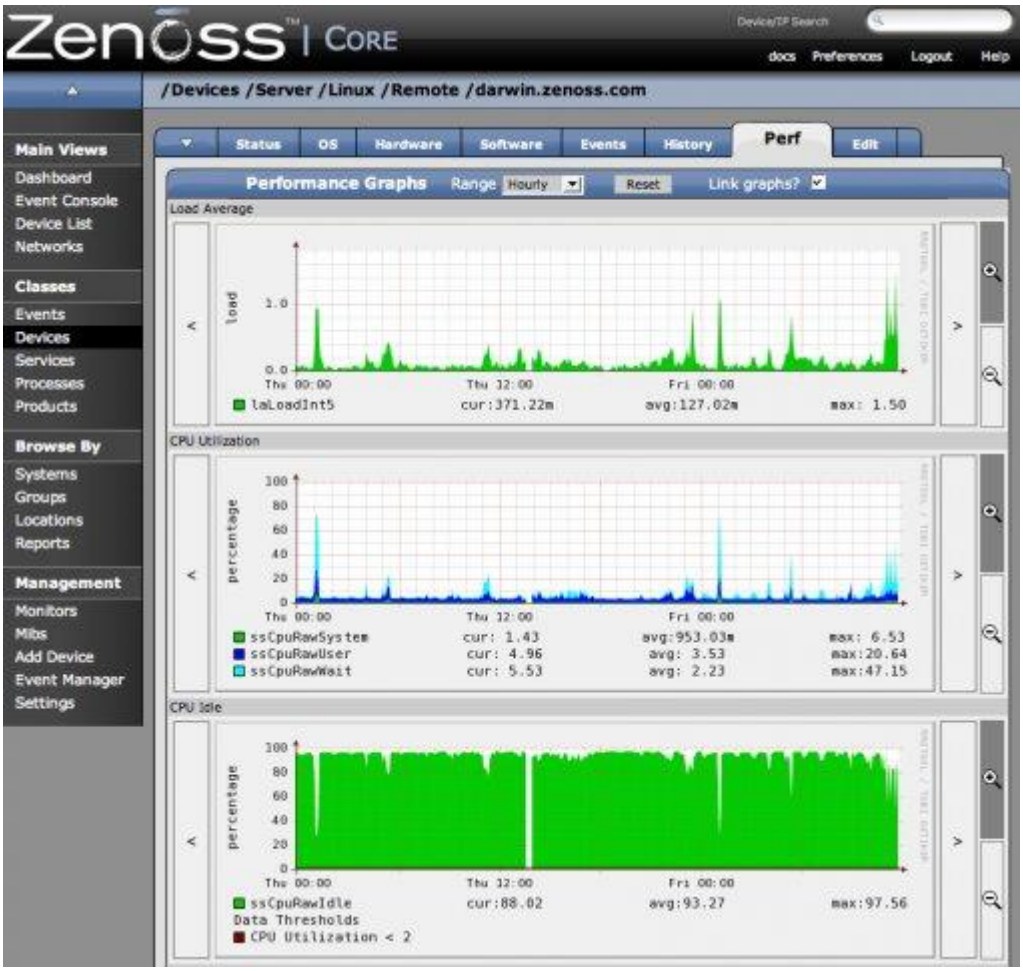
- Místo, kde jsou pluginy uloženy.

```
/usr/lib/nagios/plugins
```

### 2.11.2 Zenoss

Jedná se o komplexní dohledový systém, jehož verze Zenoss Core je k dispozici zdarma, verze Enterprise je placená. Jeho primární funkce je podobná jako u Nagiosu.

Kromě SNMP protokolu podporuje i Telnet a SSH připojení, či WMI pod Windows. Systém je postaven na principu kolektorů, které sbírají údaje a odesílají je do centrální databáze. Celé sledování je postaveno na základě dělení do tříd uspořádaných v stromě. Nastavení sledování ve vyšší vrstvě se automaticky přenáší na podtřídy (15).




**Obr. č. 18: Prostředí systému Zenoss** (Zdroj: 25)

Zenoss umí automaticky nalézt a identifikovat zařízení připojená v síti. Vychází z předpokladu, že náklady na sledování podobných zařízení je možno minimalizovat jen za využití podobných postupů. Pracuje proto s objektově založenými modely, které lze jednoduše aplikovat na každý nový objekt a případně je upravit (15).

### 2.11.3 Zabbix

Systém slouží k monitorování aktivních síťových prvků, které jsou připojeny do počítačové sítě. Je tedy možné sledovat stav a sbírat různé informace o všech zařízení, která mají IP adresu. Celý systém je tvořen serverem, agentem, webovým rozhraním pro

správu a nepovinným proxy serverem. V Zabbixu je možné definovat automatické akce, které mají být provedeny po určitém incidentu, díky tomu lze předcházet výpadkům. Po detekci anomálie Zabbix dokáže spustit automatické skripty, diagnostické skripty, restartovat službu a zaslat oznámení. Záleží na konkrétním nastavení a preferencích uživatele (13).

## 2.12 Shrnutí analýzy

Služby společnosti CPU-Kocourek, s.r.o., využívá více než polovina domácností v obci Babice nad Svitavou. Další potencionální klienty představuje developerský projekt Haas Fertigbau, který připravuje pozemky pro výstavbu 54 rodinných domů. Většina nových klientů přichází s tím, že jim byly služby doporučeny okolím, proto je pro společnost velice důležité zajistit vysokou kvalitu poskytovaných služeb, a tím si v obci udržovat dobrou pověst.

Z provedené analýzy a konzultací s poskytovatelem vyplývá, že největším nedostatkem managementu sítě je správa chyb. Chybí zde dohledový systém, který by okamžitě a v kteroukoliv dobu dokázal informovat o vzniklém problému, a tím urychlil provedení servisního zásahu.

Poskytovatel přesně definoval potřeby kladené na nově nasazovanou technologii. Tyto potřeby splňuje hned několik open source řešení Nagios, Icinga, Zenoss či případně Zabbix

# 3 Vlastní návrh řešení

Návrh zahrnuje výběr a implementaci vhodné technologie, která odstraní nedostatky zjištěné při analýze současného stavu a zároveň bude splňovat požadavky definované poskytovatelem internetového připojení společností CPU-Kocourek, s.r.o.

Z provedené analýzy vyplývá, že největším nedostatkem managementu sítě je správa chyb, především v oblasti monitoringu. Poskytovatel má sice přehled o datových tocích a připojených klientech, postrádá však systém, který by co nejrychleji upozornil na vzniklé výpadky či jiné problémy a tím urychlil jejich vyřešení.

## 3.1 Výběr vhodného řešení

Možných řešení se nabízí hned několik, proto je nutné tato řešení porovnat a vybrat to nejvhodnější. Porovnání možných řešení je znázorněno v následující tabulce.

**Tab. č. 10: Matice výběru možných řešení** (zpracováno dle (13, 24))

| | Nagios | Icinga | Zabbix | Zenoss |
|---|---|---|---|---|
| **Open source** | ✓ | ✓ | ✓ | ✓ |
| **Velké množství sledovaných prvků** | ✓ | ✓ | ✓ | ✓ |
| **Podpora SNMP** | Přes plugin | Přes plugin | ✓ | ✓ |
| **Podpora notifikací** | ✓ | ✓ | ✓ | ✓ |
| **Existence komerční verze** | X | X | X | ✓ |
| **Podpora dashboardu** | ✓ | ✓ | ✓ | ✓ |
| **Síťové mapy** | ✓ | ✓ | ✓ | ✓ |
| **Podpora IPv6** | ✓ | ✓ | ✓ | ✓ |
| **Dokumentace** | Vynikající | Dobrá | Slabá | Vynikající |
| **Jednoduchá konfigurace přes rozhraní** | X | X | ✓ | ✓ |
| **Licence** | GNU, GPL | GNU, GPLv2 | GNU, GPL | GNU, GPL |
| **Uchování dat** | Soubor, SQL | SQL, PostgreSQL, Oracle | Oracle, Mysql, PostgreSQL, SQLite | Oracle, Mysql, PostgreSQL, SQLite |
| **Mobilní aplikace** | ✓ | ✓ | ✓ | ✓ |

### 3.1.1 Shrnutí možných řešení

#### Nagios a Icinga

Nagios je kompletní monitorovací nástroj s velkým množstvím již vytvořených pluginů a přídavných aplikací, protože zde existuje obrovská podpora ze strany komunity. Jediným problémem je jeho konfigurace, protože se jedná o poměrně složitý a zdlouhavý proces. Existuje však open source aplikace Centreon, která velmi výrazně zjednodušuje konfiguraci a práci s Nagiosem.

Systém Icinga vzniknul jako alternativní větev právě Nagiosu, ale i přes realizované změny jsou si tyto systémy velmi podobné a jsou vzájemně kompatibilní.

#### Zabbix

Plnohodnotný monitorovací nástroj, který umožňuje konfiguraci přes grafické prostředí. Jedna aplikace tedy pokrývá vše potřebné, co se od monitorovacího systému očekává. Nevzniká zde potřeba udržovat více různých podpůrných aplikací, jako je tomu u Nagiosu. Nevýhodou je horší dokumentace, podpora při řešení problémů či při přidávání netriviálních kontrol a také zde chybí desktop monitor.

#### Zenoss

Velice inteligentní monitorovací nástroj, do kterého se dají implementovat pluginy z Nagiosu, což mu přidává vysokou použitelnost. Má dobrou podporu komunity a obsahuje desktop monitor. Nevýhodou je existence placené verze, protože v základu nejsou některé funkce dostupné.

### 3.1.2 Výběr konkrétního řešení

Každý systém má svoje výhody i nevýhody, proto není jednoduché jednoznačně rozhodnout o výběru, ale při prezentaci nabízených možností ve společnosti CPU-Kocourek, s.r.o. jsem na základě konzultací s vedoucích technického oddělení a jednatelem společnosti zvolil systém Nagios s podporou Centreonu. Systém splňuje veškeré požadavky a na základě výborné dokumentace, volně dostupných pluginů a znalostí zaměstnanců bude společnost sama schopna provést instalaci serveru, operačního systému, systému Nagios s jeho následnou konfigurací.

## 3.2 Technické aspekty

Na monitorované síťové infrastruktuře musí být umístěn server, na kterém poběží některá z distribucí Linuxu. Přípravu serveru, instalaci OS a systému Nagios provede vedoucí technického oddělení, který má s touto problematikou již řadu předešlých zkušeností.

### 3.2.1 Server pro monitoring

Současný server není dostatečně výkonný pro nasazení nového dohledového systému, proto navrhuji pořízení nového serveru Dell PowerEdge R220. Server disponuje následující specifikací, která bude pro chod systému Nagis zcela dostačující:

**Specifikace serveru:**

- Provedení serveru je Rack 1U
- Intel® Xeon® E3-1220 v3(3.1/3.5GHz)
- 16GB (2x8GB) paměti DDR3 s frekvencí 1600MHz, pro další růst jsou k dispozici celkem 4 sloty pro až 32GB paměti
- 2x 1TB disky SATA s rychlostí 7 200 otáček za minutu
- 1x 250W zdroj
- Připojení k síti je zajišťuje dvojice Gigabitových portů.

**Zabezpečení serveru**

Toto zabezpečení je zavedeno především proti neoprávněnému přístupu, manipulaci nebo odcizení hardware a tím zapříčinění nedostupnosti poskytovaných služeb. Navrhuji umístit server do uzamykatelného racku, který je na půdě základní školy v Babicích nad Svitavou, klíče od racku budou mít všichni zaměstnanci technického oddělení.

Budova je chráněna poplachovým zařízením a v případě potřeby přístupu mimo provozní dobu školy má technické oddělení k dispozici přístupové heslo, klíče od hlavního vchodu a půdy. Podmínkou při vstupu v této době je informování ředitelky školy a starosty obce. Přístupová hesla a jména k serveru budou mít pouze jednatel společnosti a vedoucí technického oddělení.

### 3.2.2 Operační systém

Systém Nagios je primárně vyvíjen pro Linux, proto po konzultaci s vedoucím technického oddělení navrhuji využít volně dostupnou linuxovou distribuci Ubuntu verze 9.10, která tento systém plně podporuje a existuje dostupná dokumentace pro instalaci a následnou konfiguraci.

Instalaci operačního systému provede vedoucí technického oddělení.

### 3.2.3 Instalace systému Nagios

Nagios je možné nainstalovat dvěma způsoby. Zaprvé je možné využít balíček, který je vytvořen na konkrétní distribuci, anebo lze provést instalaci z binárních souborů. Pro instalaci doporučuji druhý způsob.

Z domovské internetové stránky http://www.nagios.org/download/ je možné stáhnout balíček jádra systému, který sestává z démona a webového rozhraní a balíček, ve kterém jsou obsaženy zásuvné moduly.

Kompletní instalaci a konfiguraci systému Nagios provede vedoucí technického oddělení.

## 3.3 Definice zařízení a služeb

Nagios používá k definování testovaných zařízení a služeb tzv. objekty. Jsou to konfigurační soubory definované v konfiguračním souboru `nagios.cfg`.

**Tab. č. 11 : Objekty nagiosu** (Zdroj: 24)

| | |
|---|---|
| Definice hostů | cfg_dir=/usr/local/etc/nagios/objects/hosts.cfg |
| Definice monitorovaných služby | cfg_dir=/usr/local/etc/nagios/objects/services.cfg |
| Definice kontaktů | cfg_file=/usr/local/etc/nagios/objects/contacts.cfg |
| Definice časových intervalů | cfg_file=/usr/local/etc/nagios/objects/timeperiods.cfg |
| Definice příkazů | cfg_file=/usr/local/etc/nagios/objects/commands.cfg |
| Definice skupin hostů | cfg_file=/usr/local/etc/nagios/objects/hostgroups.cfg |

### 3.3.1 Definování zařízení (hosts)

V tomto konfiguračním souboru jsou definována veškerá zařízení, která je potřebné monitorovat. Navrhuji monitorovat páteřní spoj Brno-Babice nad Svitavou, veškeré lokální páteřní spoje, všechny vysílače a router.

**Navrhovaná definice hostů je následující:**

```
define host {
          host_name                    /název zařízení
          address                      /IP adresa zařízení
          check_command                check-host-alive
          max_check_attempts           3
          retry_interval               1
          check_interval               5
          check_period                 24x7
          contact_groups               technici
          notification_interval        60
          notification_period          24x7
          notification_options         d,u,r
           }
```

Každé zařízení je definováno jeho jménem a jeho IP adresou. Všechna zařízení budou kontrolována základní metodou *check-host-alive,* která pro svoji činnost vyžívá příkaz *check.ping.* Každé zařízení bude testováno v intervalu 5 minut, pokud dojde k chybovému vyhodnocení, tak test bude opakován po 1 minutě, když dojede k opakování testu 3x, tak Nagios vygeneruje informaci o problému.

Zasílání oznámeni o problému je nastaveno po každých 60 minutách na kontaktní skupinu technici v režimu 24/7 v případě, že zařízení je ve stavu:

- d – DOWN
- u – UNREACHABLE
- r – UP

Veškeré hodnoty jsou pouze navrhované, během testování může u některých zařízení dojít k jejich změně, dle nově vypozorovaných potřeb.

### 3.3.2 Definice testované služby (services)

Nastavování parametrů testované služby je velmi podobné jako při konfiguraci definice zařízení. Návrh některých služeb a jejich parametrů je následující:

*Client_signal* – signál klienta.

- Signál je větší než -50dB odešle se stav WARNING
- Signál je větší než -60dB odešle se stav CRITICAL
- Signál je menší než -50dB odešle se stav RECOVERY
- Pokud je služba nedostupná odešle se stav UNREACHABLE

*Clients_count* – počet připojených klientů k vysílači.

- Počet klientů je větší než 30 odešle se stav WARNING
- Počet klientů je větší než 40 odešle se stav CRITICAL
- Počet klientů je menší než 30 odešle se stav RECOVERY
- Pokud je služba nedostupná odešle se stav UNREACHABLE

*Ping* – odezva zařízení.

- Odezva zařízení je větší než 200ms odešle se stav WARNING
- Odezva zařízení je větší než 700ms odešle se stav CRITICAL
- Odezva zařízení je menší než 200ms odešle se stav RECOVERY
- Pokud je služba nedostupná odešle se stav UNREACHABLE

`check_all_disks` – kontrola volného místa na disku na serveru

- Pokud je zaplněno více než 75 % místa na disku odešle se stav WARNING
- Pokud je zaplněno více než 90 % místa na disku odešle se stav CRITICAL
- Pokud je zaplněno méně než 75 % místa na disku odešle se stav RECOVERY
- Pokud je služba nedostupná odešle se stav UNREACHABLE

Veškeré hodnoty jsou pouze navrhované, během testování může u některých služeb dojít k jejich změně, dle nově vypozorovaných potřeb.

### 3.3.3 Definice kontaktů (contacts)

V tomto konfiguračním souboru se definují kontaktní údaje o osobách, které mají být informovány o vzniklých událostech. Navrhuji definovat všechny zaměstnance technického oddělení, kterým budou zasílány notifikace na služební emaily a telefonní kontakty v režimu 24/7. Zasílány budou veškeré notifikace hostů i služeb, dle následujícího návrhu:

```
define contact {
       contact_name
       alias Nagios                        admin
       email                               admin@net4babice.cz
       pager                               +774 147 xxx
       host_notification_period            24x7
       service_notification_period         24x7
       host_notification_options           d,u,r
       service_notification_options        w,u,c,r
       host_notification_commands          notify-host-by-email/sms
       service_notification_commands       notify-service-by-email/sms
                 }
```

### 3.3.4 Definice časových intervalu odesílání notifikace (timeperiods)

V tomto kroku je nutné definovat časové intervaly, během nichž bude monitorovací systém generovat a odesílat notifikace osobám, které byly definovány v kontaktech. Navrhuji ponechat defaultní nastavení po instalaci, které je nastaveno na režim 24/7.

```
define timeperiod {
     timeperiod_name         24x7
     alias                   24 Hours A Day, 7 Days A Week
     Friday                  00:00-24:00
     Thursday                00:00-24:00
     Wednesday               00:00-24:00
     Tuesday                 00:00-24:00
     Monday                  00:00-24:00
     Sunday                  00:00-24:00
     Saturday                00:00-24:00
                 }
```

## 3.4 Testovací provoz

Testovací provoz proběhne po konfiguraci serveru a systému Nagios, cílem bude odladění nastavení monitorovaných zařízení, služeb a hodnot, při kterých budou zasílána upozornění o vzniklém problému. Testováno bude zda:

- Jsou správně nakonfigurována všechna monitorovaná zařízení a služby,
- je skutečně odesláno upozornění na všechny definované kontakty při vzniklém problému,
- nejsou odesílána zbytečná a příliš častá upozornění,
- vytížení monitorovacího serveru.

Odpovědnost za testovací provoz nese vedoucí technického oddělení. Navrhovaná doba testovacího provozu je 5 týdnů. Při potřebě prodloužení testovacího provozu schvaluje tuto skutečnost jednatel společnosti, který zároveň schvaluje uvolnění systému Nagios do rutinního provozu po ukončení testovací fáze.

## 3.5 Režim rutinního provozu

Tento režim nastane po úspěšném ukončení testovacího provozu a po schválení jednatelem společnosti. Síť bude monitorována v režimu 24/7, ve stejném režimu pak budou odesílány notifikace na definované kontakty.

### 3.5.1 Organizační začlenění technologie, odpovědnost, pravomoci

Monitorovací systém Nagios budou využívat jen zaměstnanci, spadající do technického oddělení dle organizační struktury společnosti. Jedná se o vedoucího technického oddělení a o jednotlivé techniky zajišťující montáž a servis.

Notifikace o oznámení problému budou odesílány na všechny zaměstnance technického oddělení na jejich služební email a formou sms zprávy na jejich služební telefonní číslo.

**Určení odpovědnosti za:**

- **Aktualizace systému Nagios a jeho údržba** - vedoucí technického oddělení,
- **Sledování příchozích notifikací** - zaměstnanec konající službu,

- **Vytvoření ticketu v systému RT** - zaměstnanec konající službu,
- **Provedení postupů při vzniklém problému** - zaměstnanec konající službu,
- **Evidenci provedených změn** (např. výměna zařízení, změna frekvence, přepojení uživatelů apod.) - zaměstnanec, který změnu provedl
- **Rozpis služeb** - vedoucí technického oddělení,
- **Zpracování reportů** - vedoucí technického oddělení,
- **Uzavírání vyřešených tiketů v systému RT** – vedoucí technického oddělení nebo zaměstnanec, který tiket vyřešil.

Přístup do systému bude mít pouze vedoucí technického oddělení a jednatel společnosti. Ostatní zaměstnanci technického oddělení nebudou mít přístup do systému, budou pouze přijímat příchozí notifikace a nebudou moci zasahovat do konfiguračních souborů.

### 3.5.2 Návrh postupů pro technické oddělení (směrnice)

V této kapitole jsou popsány postupy, které je nutné dodržovat při obdržení některé z notifikací zaslaných systémem Nagios. Při vzniklém problému je vždy zaměstnanec konající službu povinen založit tiket v systému RT.

1. **Notifikace monitorovaných hostů (kontrola *`check-host-alive`*)**

**Páteřní spoj Brno – Babice nad Svitavou**

Při výpadku hlavního spoje je nastaveno okamžité automatické přepnutí na záložní spoj, při korektním přepnutí a obnovení konektivity dojde k ohlášení vzniklého problému.

- **Host DOWN** - došlo k výpadku hlavního páteřního spoje a přepnutí na záložní spoj. Zaměstnanec konající službu zjistí příčinu výpadku a vytvoří o události tiket v systému RT, kontaktuje vedoucího technického oddělení a na základě zjištěného problému je okamžitě zahájeno řešení situace. Veškeré informace jsou uváděny do vytvořeného tiketu.
- **Host UNREACHABLE** - nedostupnost hlavního páteřního spoje, postup podobný jako u výpadku.

Pokud dojde ke korektnímu přepnutí na záložní spoj, tak nedojde k dlouhodobějšímu výpadku poskytovaných služeb.

- **Host UP** - došlo k obnově hlavního páteřního spoje a zpětnému přepnutí ze záložního spoje. Vedoucí technického oddělení uzavře tiket s informací o jeho vyřešení.

**Lokální páteřní spoj**

- **Host DOWN** - došlo k výpadku lokálního páteřního spoje, dle síťové mapy jde okamžitě poznat, o kterou větev sítě se jedná. Zaměstnanec konající službu vytvoří tiket o vzniklém problému, aktivuje záložní spoj a provede kontrolu, zda byla konektivita obnovena. Oprava spoje bude provedena následující pracovní den, veškeré informace jsou zapisovány do vytvořeného tiketu.
- **Host UNREACHABLE** - nedostupnost lokálního páteřního spoje, postup podobný jako u výpadku.
- **Host UP** - došlo k obnově lokálního páteřního spoje. Vedoucí technického oddělení uzavře tiket s informací o jeho vyřešení a deaktivuje záložní spoj.

Pokud dojde ke korektnímu přepnutí na záložní spoj, tak nedojde k dlouhodobějšímu výpadku poskytovaných služeb.

**Vysílač**

- **Host DOWN** - oznamuje výpadek některého z vysílačů a tím nedostupnost služeb všech zákazníků k němu připojených. Zaměstnanec konající službu vytvoří tiket o výpadku příslušného vysílače. Tyto výpadky jsou v pracovní době řešeny okamžitě, v jiném případě následující den.
- **Host UNREACHABLE** - nedostupnost vysílače, opět postupy podobný jako u výpadku.
- **Host UP** - vysílač je opět dostupný. Zaměstnanec, který sjednal nápravu, tiket uzavře s komentářem o jeho vyřešení.

Při výpadku některého z vysílačů je zaslán omluvný email o nedostupnosti poskytovaných služeb všem zákazníkům, kterých se tento problém týkal.

**Router**

- **Host DOWN** - pokud dojde k výpadku routeru, tak zaměstnanec konající službu založí tiket o vzniklém problému a je potřeba okamžitě zjistit proč k výpadku došlo a ihned zajistit opravu. V případě potřeby má technické oddělení k dispozici náhradí router.
- **Host UNREACHABLE -** nedostupnost routeru, postup podobný jako u výpadku.
- **Host UP** – router je opět dostupný a zaměstnanec, který sjednal nápravu, tiket uzavře s komentářem o jeho vyřešení.

**Monitorovací server**

Dojde-li ke zjištění výpadku monitorovacího serveru se systémem Nagios, tak zaměstnanec konající službu založí tiket a okamžitě kontaktuje vedoucího technického oddělení, který se bude vzniklým problémem zabývat. Pokud dále nedojde k jiným výpadkům, tak problémy s monitorovacím serverem nepředstavují vážnější dopad na úroveň poskytovaných služeb.

2. **Notifikace o monitorovaných službách**

Pokud dojde z některého hosta hlášení **WARNING** o některé z monitorovaných služeb a problém přetrvává u stejného hosta delší dobu, tak zaměstnanec konající službu vytvoří tiket, ve kterém bude problém řešen v pracovní době, protože se nejedná o kritickou situaci. Pokud dojde z některého hosta hlášení **CRITICAL** o některé z monitorovaných služeb a problém přetrvává u stejného hosta delší dobu, tak zaměstnanec konající službu opět vytvoří tiket, řešení situace je zahájeno v co nejblíže možné době.

Dojde-li z některého hosta hlášení **RECOVERY** o některé z monitorovaných služeb, tak je služba již v pořádku. Pokud k dříve vzniklému problému existuje vytvořený tiket, tak zaměstnanec, který sjednal nápravu, tiket uzavře s komentářem o jeho vyřešení.

## 3.6 Projekt zavedení dohledového systému

### 3.6.1 Identifikační listina

Zahájení projektu předchází vypracovaní a schválení identifikační listiny, která je jeho základním dokumentem.

| | |
|---|---|
| **Název projektu:** | Implementace nového dohledového systému |
| **Druh projektu:** | Interní projekt společnosti |
| **Cíl:** | Zavedením dohledového systému zkvalitnit úroveň v oblasti poskytování datových služeb, konkrétně v rychlosti řešení výpadků. |
| **Výstupy:** | Implementace dohledového systému<br>Zvýšení úrovně poskytovaných služeb |
| **Plánovaný termín zahájení:** | 01. 02. 2016 |
| **Plánovaný termín ukončení:** | 01. 04. 2016 |
| **Plánované náklady:** | 38 000 Kč |
| **Projektový tým:** | Jednatel společnosti<br>Vedoucí technického oddělení |
| **Místo realizace:** | Obec Babice nad Svitavou |

**Milníky projektu**

**Tab. č. 12 : Milníky projektu** (Zdroj: Vlastní zpracování)

| Název milníku | Termín milníku |
|---|---|
| **Zahájení projektu** | 01. 02. 2016 |
| **Zajištěn HW a SW** | 11.02 2016 |
| **Konfigurace a testování** | 20. 03. 2016 |
| **Vyhotoveny směrnice a postupy** | 25. 03. 2016 |
| **Zahájení ostrého provozu** | 31. 03. 2016 |
| **Ukončení projektu** | 1.04 2016 |

### 3.6.2 Časový harmonogram projektu

Realizace je naplánována na první polovinu roku 2016, protože v tomto období není pánována žádná další modernizace sítě ani další činnosti, které by mohly ovlivňovat tento projekt.

Během realizace může dojít k mírné úpravě sestaveného harmonogramu, byl však sestaven tak, aby při realizaci nedocházelo, nebo jen minimálně, ke zpoždění daných úkolů. Časy zahájení a ukončení jednotlivých činností jsou odhadovány na základě konzultací s vedoucím technického oddělení.

Termín zahájení je 1. 2. 2016 a termín ukončení je naplánován na 1. 4. 2016, zodpovědnost za dodržování termínů má vedoucí technického oddělení.

**Tab. č. 13: Harmonogram projektu** (Zdroj: Vlastní zpracování)

| Úkol | Zahájení | Dokončení |
|---|---|---|
| **Zavedení dohledového systému** | **1.2.2016** | **1.4.2016** |
| | | |
| **Příprava serveru** | **1.2.2016** | **11.2.2016** |
| **Objednávka** | 1.2.2016 | 2.2.2016 |
| **Doručení** | 2.2.2016 | 8.2.2016 |
| **Zprovoznění a instalace OS** | 8.2.2016 | 9.2.2016 |
| **Instalace systému Nagios** | 9.2.2016 | 10.2.2016 |
| **Umístění do racku v Obci Babice nad Svitavou** | 10.2.2016 | 11.2.2016 |
| **Implementační fáze** | **11.2.2016** | **31.3.2016** |
| **Konfigurace** | 11.2.2016 | 14.2.2016 |
| **Nastavení metrik** | 14.2.2016 | 15.2.2016 |
| **Testovací provoz a ladění metrik** | 15.2.2016 | 20.3.2016 |
| **Ladění směrnic a postupů** | 20.3.2016 | 25.3.2016 |
| **Školení** | 25.3.2016 | 30.3.2016 |
| **Zavedení do ostrého provozu** | 31.3.2016 | 31.3.2016 |
| **Vyhodnocení projektu** | **1.4.2016** | **1.4.2016** |
| **Ukončení projektu** | **1.4.2016** | **1.4.2016** |

## 3.7 Ekonomické aspekty

### 3.7.1 Náklady

Náklady na nasazení systému Nagios jsou tvořeny především pořízením nového serveru. Protože se jedná o open source řešení, které poběží na volně dostupné linuxové distribuci Ubuntu verze 9.10, nemusí se platit žádné licenční poplatky.

Instalaci operačního systému, Nagiosu a následnou konfiguraci monitorovaných zařízení a služeb provede vedoucí technického oddělení v pracovní době.

| | |
|---|---|
| **Pořízení serveru:** | 32 387 Kč |
| **Vypracování projektu:** | 3 000 Kč |
| **Instalace OS a Nagios:** | Vedoucí technického oddělení v pracovní době |
| **Konfigurace:** | Vedoucí technického oddělení v pracovní době |
| **Celkové náklady:** | 35 387 Kč |

### 3.7.2 Přínosy pro firmu

Společnost CPU-Kocourek, s.r.o., poskytuje bezdrátové internetové připojení a je nutné mít okamžitý přehled nad stavem sítě a reagovat na vzniklé problémy. Systém Nagios velmi rychle informuje o vzniklém problému a zaměstnanci technického oddělení, tak mohou co nejdříve zahájit potřebné kroky k jeho nápravě.

Rychlost provádění servisních zásahů vede ke zlepšování kvality poskytovaných služeb a tím i k zvyšování spokojenosti připojených zákazníků, což je pro společnost jedním z nejdůležitějších faktorů.

# Závěr

Cílem této diplomové práce bylo vybrat a implementovat vhodnou technologii pro poskytovatele internetového připojení v obci Babice nad Svitavou. Na základě provedené analýzy současného stavu bylo zjištěno, že největším nedostatkem managementu počítačové sítě je správa chyb, především v oblasti monitoringu. Technické oddělení sice má přehled o datových tocích a připojených klientech, postrádá však systém, který by co nejrychleji upozornil na vzniklé výpadky či jiné problémy a tím urychlil jejich vyřešení.

Vedoucí technického oddělení definoval potřeby, které byly rozhodující pro výběr nejvhodnějšího řešení. Možných alternativ se nabízelo hned několik, z nichž byl nakonec zvolen systém Nagios s podporou Centreonu. Hlavním důvodem výběru byla existence odborné dokumentace, na jejímž základě si společnost bude sama schopna provést instalaci a následnou konfiguraci zvoleného řešení.

V návrhu jsou zahrnuty technické aspekty, které jsou nezbytné pro úspěšnou implementaci systému Nagios, jedná se především o návrh nového serveru s doporučeným operačním systémem. V další fázi jsou navrhnuty zařízení a služby, které je potřeba monitorovat, včetně hodnot, při kterých bude zasíláno upozornění na definované kontakty.

Pro zahájení projektu implementace systému Nagios byla vytvořena identifikační listina a časový harmonogram projektu, který schvaluje jednatel společnosti. Ekonomické zhodnocení obsahuje náklady vynaložené při realizaci projektu.

Hlavním přínosem zavedení systému Nagios je urychlení provádění servisních zásahů při vzniklém problém, a tím zvyšování úrovně poskytovaných služeb.

# Seznam použité literatury


(1) ZLATUŠKA, J. *Informační společnost*. Zpravodaj ÚVT MU. ISSN 1212-0901, 1998, roč. VIII, č. 4, s. 1-6.

(2) HLADKÁ, E. a FOUSEK, J. *Základy IT gramotnosti* [Online]. © 2015 [cit. 2015-12-18]. Dostupné z: http://is.muni.cz/do/1492/el/sitmu/law/html/odpovednost-isp.html

(3) PUŽMANOVÁ, R. *Moderní komunikační sítě od A do Z*. 2. vydání. Brno: Computer Press, 2006. 432 s. ISBN 80-251-1278-0

(4) SENSE. Optický kabel. *sense.cz* [Online]. © 2013 [cit. 2015-12-19]. Dostupné z:http://www.sense.cz/files/image/P06_optick%C3%BD_kabel_multimode.jpg

(5) KASSEX. *Jak na to?: Profesionální datové komunikace strukturované a multimediální kabeláže*. Kroměříž: Kassex, 2005.

(6) DOLEŽAL, M. *Návrh univerzální kabeláže pro společnost GNT s.r.o.* Brno: Vysoké učení technické v Brně, Fakulta podnikatelská, 2013. 57 s. Vedoucí bakalářské práce Ing. Viktor Ondrák, Ph.D.

(7) ZANDL, P. *Bezdrátové sítě Wi-Fi: Praktický průvodce.* 1. vyd. Brno: Computer Press, 2003. 190 s. ISBN 80-7226-632-2

(8) KÖHRE, T. *Stavíme si bezdrátovou síť Wi-Fi*. 1. vyd. Brno: Computer Press, 2004. 297 s. ISBN 80-251-0391-9

(9) SOSINSKY, B. *Mistrovství - počítačové sítě.* Brno: Computer Press, 2010. 840 s. ISBN 978-80-251-3363-7.

(10) 3.BP. Model FCAPS. *3.bp.blogspot.com* [Online]. © 2015 [cit. 2015-12-19]. Dostupné z: http://3.bp.blogspot.com/-lVSYxkC7PV4/UYkvcUGYzQI/AAAAAAAAAAo/KAHJtyPp_9U/s1600/fcaps.jpg

(11) BIGELOW, S. J. *Mistrovství v počítačových sítích: správa, konfigurace, diagnostika a řešení problémů.* 1. vydání. Praha: Computer Press, 2004. 990 s. ISBN 80-251-0178-9.

(12) CLEMM, A. *Network management fundamentals.* 1. vydání. Indianapolis: Cisco Press, 2007. 552 s. ISBN 1-58720-137-2.

(13) KRETCHMAR, J. M., DOSTÁLEK, L. Administrace a diagnostika sítí: pomocí OpenSource utilit a nástrojů. 1. vydání. Brno: Computer Press, 2004. 216 s. ISBN 80-251-0345-5.

(14) GAMEPUB. Struktura MIB. *files.gamepub.sk* [Online]. © 2015 [cit. 2015-12-19]. Dostupné z: http: http://files.gamepub.sk/statnice/RTS/skuska-vycuc/struktura_mib.png

(15) HORÁK, J. a KERŠLÁGER, M. *Počítačové sítě pro začínající správce.* 5. vydání. Brno: Computer press, 2011. 304 s. ISBN 978-80-251-3176-3.

(16) WIKIPEDIA. Schéma moderní NetFlow architektury. *cs.wikipedia.org* [Online]. © 2015 [cit. 2015-12-20]. Dostupné z: https://upload.wikimedia.org/wikipedia/commons/c/cb/NetFlowModerniArchitektura.png

(17) SCHWALBE, K. *Řízení projektu v IT.* 1. vydání. Brno: Computer Press, 2011. 623 s. ISBN 978-80-251-2882-4.

(18) I4WIFI. Katalog produktů Ubiquiti. *i4wifi.cz* [Online]. © 2015 [cit. 2015-12-20]. Dostupné z: http://www.i4wifi.cz/Ubiquiti-NS-Bullet/

(19) I4WIFI. Katalog produktů MikroTik. *i4wifi.cz* [Online]. © 2015 [cit. 2015-12-20]. Dostupné z: http://www.i4wifi.cz/MikroTik-RouterBoardy/

(20) FLYFOTO. Letecké snímky. *flyfoto.cz* [Online]. © 2015 [cit. 2015-12-29]. Dostupné z http://www.flyfoto.cz/2014/04/babice-nad-svitavou.html

(21) TS-HYDRO. Nabídka tarifů Babice nad Svitavou. *kanice.net* [Online]. © 2015 [cit. 2015-12-30]. Dostupné z: http://www.kanice.net/index.php?page=babice

(22) MAXTRON. Tarify určené pro internetové připojení Babice nad Svitavou. *maxtron.cz* [Online]. © 2014 [cit. 2015-12-30]. Dostupné z: http://www.maxtron.cz/internet-babice

(23) RYWASOFT. Bezdrátový internet v Brně a okolí *rywasoft.net* [Online]. © 2015 [cit. 2015-12-30]. Dostupné z: http://www.rywasoft.net/internet.php

(24) Ubuntu. Nagios. *Wiki.ubuntu.cz* [Online]. © 2013 [cit. 2015-08-15]. Dostupné z: http://wiki.ubuntu.cz/nagios

(25) OSTATIC. Zenoss Core Enterprise IT. *ostatic.com* [Online]. © 2015 [cit. 2015-08-15]. Dostupné z: http://ostatic.com/files/images/Zenoss%20Core%20-%20 Enterprise%20IT%20Monitoring(2).jpg

# Seznam obrázků

**Obr. č. 1: Optický kabel ..... 16**

**Obr. č. 2: Kabel kroucených párů UTP / FTP ..... 18**

**Obr. č. 3: Model FCAP ..... 22**

**Obr. č. 4: Zasílání SNMP zpráv ..... 29**

**Obr. č. 5: Struktura MIB ..... 31**

**Obr. č. 6: NetFlow architektura ..... 35**

**Obr. č. 7: Logo sítě NET4BABICE ..... 38**

**Obr. č. 8: Organizační struktura společnosti CPU-Kocourek s.r.o. ..... 39**

**Obr. č. 9: Mapa sítě ..... 41**

**Obr. č. 10: Páteřní spoj z lokality Brno-Lesná ..... 42**

**Obr. č. 11: UBIQUITI PowerBeam M5 400 AirMAX ..... 43**

**Obr. č. 12: MikroTik CCR1016-12G ..... 44**

**Obr. č. 13: NanoStation M5 Loco AirMAX ..... 45**

**Obr. č. 14: Náhled do uživatelského prostředí programu WinBox ..... 47**

**Obr. č. 15: Náhled do webového rozhraní aplikace AirControl ..... 47**

**Obr. č. 16: Letecký snímek obce z roku 2012 ..... 48**

**Obr. č. 17: Logo Nagios Core ..... 55**

**Obr. č. 18: Prostředí systému Zenoss ..... 57**

# Seznam tabulek

**Tab. č. 1: Kategorie komponent metalické kabeláže a třídy použití sítě ..... 17**

**Tab. č. 2: Standardy IEEE 802.11 ..... 19**

**Tab. č. 3: Raci matice ..... 40**

**Tab. č. 4: Specifikace produktu PowerBeam M5 400 AirMAX ..... 43**

**Tab. č. 5: Specifikace produktu NanoStation M5 Loco AirMAX ..... 45**

**Tab. č. 6: Nabízené tarify platné k 1.1.2015 ..... 49**

**Tab. č. 7: Nabízené tarify TS-Hydro platné k 1.1.2015 ..... 50**

**Tab. č. 8: Nabízené tarify Maxtron platné k 1.1.2015 ..... 51**

**Tab. č. 9: Nabízené tarify RYWASOFT platné k 1.1.2015 ..... 51**

**Tab. č. 10: Matice výběru možných řešení ..... 59**

**Tab. č. 11 : Objekty nagiosu ..... 62**

**Tab. č. 12 : Milníky projektu ..... 70**

**Tab. č. 13: Harmonogram projektu ..... 71**

# Seznam příloh

**Příloha č. 1:** Výpis monitorovaných hostů

## Příloha č. 1: Výpis monitorovaných hostů

| Host | Status | Last Check | Duration | Status Information |
|---|---|---|---|---|
| mikrotik-Kratochvilova | UP | 01-04-2016 20:25:06 | 20d 20h 7m 0s | PING OK - Packet loss = 0%, RTA = 3.10 ms |
| mikrotik-ben-skola | DOWN | 10-19-2015 20:49:08 | 83d 5h 1m 35s | CRITICAL - Host Unreachable (10.8.163.23) |
| mikrotik-has-skola | UP | 01-04-2016 20:23:06 | 23d 8h 14m 42s | PING OK - Packet loss = 0%, RTA = 3.59 ms |
| mikrotik-kocourek | UP | 01-04-2016 20:25:06 | 20d 20h 7m 0s | PING OK - Packet loss = 37%, RTA = 2.55 ms |
| mikrotik-krivonozka | UP | 01-04-2016 20:22:56 | 3d 3h 19m 50s | PING OK - Packet loss = 0%, RTA = 2.46 ms |
| mikrotik-main | UP | 01-04-2016 20:25:06 | 20d 20h 8m 22s | PING OK - Packet loss = 0%, RTA = 0.41 ms |
| mikrotik-pan-skola | UP | 01-04-2016 20:23:46 | 20d 20h 8m 22s | PING OK - Packet loss = 0%, RTA = 5.96 ms |
| mikrotik-seh-skola | UP | 01-04-2016 20:25:36 | 3d 3h 22m 30s | PING OK - Packet loss = 0%, RTA = 9.01 ms |
| mikrotik-skola-hasgnet2 | DOWN | 09-21-2015 20:25:08 | 122d 3h 36m 31s | CRITICAL - Host Unreachable (10.8.163.27) |
| mikrotik-skola-star-tom | UP | 01-04-2016 20:25:06 | 20d 20h 7m 10s | PING OK - Packet loss = 0%, RTA = 1.25 ms |
| mikrotik-skola-stred | UP | 01-04-2016 20:25:06 | 20d 20h 8m 32s | PING OK - Packet loss = 0%, RTA = 1.16 ms |
| mikrotik-skola12 | UP | 01-04-2016 20:25:06 | 20d 20h 8m 32s | PING OK - Packet loss = 0%, RTA = 0.93 ms |
| mikrotik-skola52 | UP | 01-04-2016 20:25:06 | 20d 20h 8m 32s | PING OK - Packet loss = 0%, RTA = 0.92 ms |
| mikrotik-skolaQNET | UP | 01-04-2016 20:22:56 | 83d 4h 55m 5s | PING OK - Packet loss = 0%, RTA = 0.83 ms |
| mikrotik-star-skola | UP | 01-04-2016 20:22:56 | 20d 20h 7m 0s | PING OK - Packet loss = 0%, RTA = 3.33 ms |
| mikrotik-stred-skola | UP | 01-04-2016 20:22:56 | 3d 3h 19m 40s | PING OK - Packet loss = 0%, RTA = 2.45 ms |
| mikrotik-stred245 | UP | 01-04-2016 20:22:56 | 3d 3h 19m 50s | PING OK - Packet loss = 0%, RTA = 1.99 ms |
| mikrotik-tom-skola | UP | 01-04-2016 20:25:46 | 9d 4h 43m 50s | PING OK - Packet loss = 0%, RTA = 3.01 ms |
| miracle-kovoterm | UNREACHABLE | 01-04-2016 20:23:16 | 104d 6h 53m 35s | (Host Check Timed Out) |
| miracle-skola | DOWN | 01-04-2016 20:22:56 | 20d 20h 8m 12s | CRITICAL - Host Unreachable (10.0.0.10) |
| router-netbox | UP | 01-04-2016 20:25:06 | 20d 18h 21m 30s | PING OK - Packet loss = 0%, RTA = 1.51 ms |
| server-hlavni | UP | 01-04-2016 20:22:56 | 252d 4h 22m 11s | PING OK - Packet loss = 0%, RTA = 0.12 ms |
| server-mail | UP | 01-04-2016 20:22:56 | 625d 22h 51m 34s | PING OK - Packet loss = 0%, RTA = 0.13 ms |
| server-monitor | UP | 01-04-2016 20:22:56 | 629d 1h 8m 16s | PING OK - Packet loss = 0%, RTA = 0.12 ms |

Zdroj: (Vlastní)